PhD - DOLGOZAT

Dr. Nagy Zoltán

2000

AZ INFORMATIKAI BŰNCSELEKMÉNYEK

PhD-dolgozat

Készítette: Dr. Nagy Zoltán

Pécs, 2000.

TARTALOMJEGYZÉK

BEVEZETÉS

Vajon van-e más olyan találmánya az emberiségnek, amely alapjaiban változtatta meg élet- és munkakörülményeinket, szokásainkat, hanem egész gondolkodásunkat. A "virtuális valóság" mára olyan illúziót kelt, mintha a számítógép kezelője részese lenne az általa teremtett világnak. Közhely az, hogy a számítógép egyszerre áldás és átok.

A számítógépet övező félelem, néhány évtizede még oly' jellemző misztikum talán oldódik. Ámulunk lehetőségein, amely azonban emberi ötletekből, tudásból fakad. Nézünk rá, „mint, csodára nézni illik", mert megszeppenünk saját képességeinkkel összevetve.

Alkalmazásának fontossága, szükségessége ma már elvitathatatlan. Az elektronikus adatfeldolgozás- és adatátvitel nyújtotta előnyöket mindennapi életünkben szinte észre sem vesszük, természetesnek tartjuk. A számítógép egyszerre van jelen mindennapi munkánkban. Teret hódít otthonainkban is. Elképzelhetetlen áldásos segítsége a közigazgatásban, a vállalatok ipari tevékenységének automatizálásában, számvitelében, a közlekedésben, a távközlésben, a szállításban, a hadiiparban, az oktatásban, a tudományos kutatásban, az egészségügyben és másutt, életünk valamennyi szférájában. Vásárlási, pénzkezelési szokásainkat is átformálja. Kedvünkre száguldozhatunk, igaz borsos áron a számítógépes "szupersztrádán". Hozzáférhetünk távoli országok adatállományaihoz, vásárolhatunk árut, szolgáltatást, részesei lehetünk nemzetközi konferenciáknak, küldhetünk üzenetet egy másik kontinensen élő ismerősnek vagy ismeretlennek, és végeláthatatlanul bolyonghatunk az egyelőre szabályozatlan cyber - térben, amelyre a „pénz" már kivetette hálóját.

1. TECHNIKA-TÖRTÉNETI ÁTTEKINTÉS

A számítógépet képzeljük el olyan hatalmas *épületnek*, amelynek tégláit évszázadok tudása illeszti egybe mérnöki pontossággal.

E téglák viszont folyamatosan cserélődnek úgy, hogy az *építmény egyre kisebb lesz kívülről és egyre nagyobb „belülről"*.

A számítógép történetéről több tanulmány látott már napvilágot. Számomra szimpatikus az a felfogás, amely többirányú elméleti - gondolati és praktikus vonulat együttes, egymásra épülő fejlődéseként szintetizálja a számítógép születését.[1]

Az **első két** egyszersmind együtt haladó **ág** a számítás módszereinek és az azt segítő technikai eszközöknek a fejlődése. A XII. században egy arab matematikus *Muza al-Chavrizmi* kidolgozza az algoritmuselmélet alapjait a latinra fordított "Algoritmi dicit" c. könyvében.

Az eszközfejlesztést a fogaskerekes számológépek ötleteitől (pl. a német *W. Shickard* 1623-ban írt feljegyzésétől) és készítésétől számíthatjuk. *Leonardo da Vinci* (1452-1529), majd *B. Pascal* (1623-62), *G. W. von Leibnitz* (1646-1716) és mások is kísérleteznek a számolást megkönnyítő mechanikus gépek létrehozásával.

A másik **ág** fejlődését az ipari termelés gépesítése, majd hatékonyságának növelése indukálja. A szövőgépekhez a francia *Falcon* (1705-65) lyukasztott hengert 1725-ben, majd *J.-M. Jacquard* (1752-1834) lyukkártyát szerkeszt.

A német *H. Hollerith* (1860-1929) az 1880-as egyesült államokbeli népszámlásához lyukkártyagép-rendszert alkot és ennél is maradandóbb tényked az általa 1896-ban alapított Computing Tabulating Company, amely az IBM., mint

---

[1] Szűcs Ervin: A számítógép tegnaptól holnapig. Budapest, 1987. 35-42.l.

A MacBride jelentés. Budapest, 1983. 23-25.l.

Balogh László: Számítástechnikai alapismeretek. Debrecen, 1988. 12-15.l.

Csajbók Zoltán: A számítástechnika története (Számítástechnikai oktatási füzetek 21. száma) 1991. 5-54.l.

mára meghatározó számítógépgyártó világcég elődje. E két vonulat eredményeit a számítógép "atyjának" nevezett skót *Charles Babbage* (1792-1871) egyesíti az általa álmodott "analitikai gépben", amelyhez a lyukkártyákat kolleginája *Ada Lovelace* (1815-1852) készít.

A negyedik **ág**, amely már a számítógépek kommunikációjáig vezet, az információátviteli technika fejlődése. A francia *C. Chappe* (1763-1805) majd két évezreddel Hannibál jelzőtornyaiból álló hírközlő hálózat alkalmazása után újra felfedezi, majd megépíti a három mozgatható karból üzenettovábbító berendezést Párizs és Lille között. Az orosz *P.L. Silling* (1786-1837) villamos távjelző vonalat építtet Pétervár és Péterhof közt. Az angol *Ch. Wheatstone* (1802-75) az elektromos telegráfot, míg a német *K.F. Gauss* (1777-1855) és *W. Weber* (1804-91) az elektromos távírót szerkeszt.

Az angol *D. Hughes* (1831-1900) a betűnyomó táviratozógépet. A nagy teljesítményű gyorstávíró "nagy ötlete" magyar *Pollák Antal* (1865-1943) és *Virág József* (1870-1901) kettősnek jut eszébe.

Az információátvitelben jelentős találmány a telefon, amely az amerikai *A.G. Bell* (1847-1922) nevéhez fűződik. A telefonközpont honfitársunk *Puskás Tivadar* (1844-1893) remeke.

A telexgép és az automata ismétlő telegráf a menlo-parki varázsló *T. A. Edison* (1847-1931) ötlete. A német *H. Hertz* (1857-94) miután felfedezi a rádióhullámokat az orosz *A. Sz. Popov* (1859-1906) megépíti a rádiótávírót.

Az első és egy nagyobb szoba méretű elektromechanikus számítógépet, a Z1-et, a német *K. Zuse* (1910-) szerkeszti 1934-ben. A Z1-et további három gép követi. Néhány évvel később az óceán túlsó partján egymástól függetlenül két team alkot ilyen masinákat. A katonai - hadászati célokat is szolgáló MARK gépeket a *H. Aiken* (1900-1973), a MODEL I-IV. jelzésű masinákat *G.R. Stibitz* vezette csapat alkotja meg.

Az első elektronikus számítógépet az amerikai *J.P. Eckert* (1919-), *J.W. Mauchly* és *H.H. Goldstine* tervei alapján épül és az ENIAC (Electronic Numerical Integrator and Computer) nevet viseli.

A mai modern számítógép elvi felépítésének, logikai rendszerének nagyszerűsége a magyar származású *Neumann Jánosé* (1903-1957), aki Goldstine-nal 1944-ben kezdi építeni az EDVAC-ot (Electronic Discrete Variable Automatic Computert).

Angliában *M.V. Wilkes* (1913-) vezette csoport 1946-49 között kifejleszti az EDSAC (Electronic Delay Storage Automatic Calculator) jelű gépet. Az USA-ban az Eckert és Mauchly a BINAC (Binary Automatic Computer) betűjelű, majd az UNIVAC (Universal Automatic Computer) elnevezésű gépet alkotják meg, amely 1951-ben készült el. Az UNIVAC gép az alapja az ipari méretekben, nagy szériában gyártott számítógépeknek.

Az elektroncsöves ENIAC megjelenésétől számítjuk a számítógépek első generációját, amelyet *W. Shockley* (1910-), *J.Bardeen* (1908-1991) és *W. Brattain* (1902-1987) amerikai tudósok által kitalált tranzisztorok, valamint diódák és ferritgyűrűk felhasználásával készült második generációs gépek korszaka követ, majd a *J. Kilby* alkotta integrált áramkörök felhasználásával készült számítógépek jelentik a harmadik generációt, míg az INTEL által 1971-ben piacra dobott mikroprocesszorokkal már a számítógépek technika történetének negyedik generációja épül.

Az első mikroszámítógép, az ALTAIT 8800. 1975-ben jelenik meg, amely csupán a hobbisták és a sznobok számítógépe.

A számítógépek sikersztorija 1977-ben veszi kezdetét. Az amerikai *S. Wozniak* és *S. Jobs* egy garázsban "összedobott" APPLE nevű masinával lepi meg a világot, amelyet az 1984-es Macintosh I. és az 1987-es Macintosh II. követ. A Macintosh utánzatai a jó emlékű Commodore és Atari gépek. Természetesen a konkurencia sem tétlenkedik. Az angol *C. Sinclar* (1940-) 1980-ban piacra dobja a ZX 8O-as gépét.

Míg az IBM 1981-ben lepi meg a világot nemes egyszerűséggel PC-nek nevezett gépével. 1983-ban az IBM PC/XT (extended, vagyis bővített változat) majd egy évvel később az AT (advanced technology, azaz fejlett technológia) széria indul világhódító útjára.

Az ötödik generációt nyolcvanas évektől a VLSI (Very Large Scale Integration), azaz a nagyon nagy méretű integrálás korszaka jelenti. Mára az ULSI (Ultra Large Scale Integration) azaz az ultra nagy méretű integrálás korszakába lépünk.

Ugyanakkor e méretében csökkenő, egyre nagyobb teljesítményű gépek összekapcsolódnak és az adott intézményen, vállalaton belül belső hálózatot (intranetet), valamint ügyfeleivel, bankjával kiépített hálózaton (extraneten) tartja a kapcsolatot, vagy csatlakozik a világhálóra, az Internetre.

Az Internetet is a katonai kutatás hívja életre. A hidegháború idején a volt szovjet hatalom szputnyikot bocsát fel, az Amerikai Védelmi Minisztérium erre válaszként életre hívja Fejlett Kutatási Program Ügynökséget (Advance Research Project Agency). Ez az ügynökség 1969-ben létrehozza az első nagyszámítógépes hálózatot.

A hetvenes években kutatóintézetek, egyetemek is csatlakoznak a hálózathoz. Ekkor már a hálózat ARPA-Internetté alakul át, ám a rendszer irányítása a Pentagon kezében marad.

1976-ban II. Erzsébet küldi az első elektronikus üzenetet (e-mailt). Az ezt követő évben az e-mailt szabványosítják.

1982-ben létrejön az EUNET, az első európai Internet szolgáltatás Nagy-Britanniában, Hollandiában, Dániában, Svédországban, majd másutt is.

1985-86-ban az ARPA-Internet MILNET-re (Military Network - Katonai Hálózat) és Internetre bomlik.

1991-ben az amerikai Nemzeti Kutatási Alapítvány engedélyt ad az Internet kereskedelmi célú hasznosítására. Napjainkban az elektronikus kereskedelem nemcsak az üzletemberek egymás közötti kapcsolatait (pl. a szerződéskötést) gyorsítja (business to business), hanem az ügyfelek teljesebb és gyorsabb kiszolgálását (business to consumer) is lehetővé teszi.

Virtuális áruházak nyílnak a világhálón, amelyek szélesebb választékkal, és kevesebb hálózati költséggel kínálják portékait, mint a hagyományos áruházak.

Vásárolni bankkártyával (on-line), vagy utánvéttel illetőleg futárszolgálat útján (off-line) lehet.

A telebank-szolgáltatás keretében a bankok ügyfeleik számára lehetővé teszik átutalások, betétlekötések, befektetések, hitelkérelmek, és más pénzügyi műveletek teljesítését.

Minden bizonnyal majdan a közigazgatás, és az ügyfelek kapcsolata is a világhálón keresztül zajlik: pl. az állampolgárok adatainak bejelentése, módosítása, lakcímbejelentés, okmányok igénylése, érvényesítése

Tele- vagy távmunka olyan előnyöket rejt (kevesebb iroda, kisebb rezsi költség, az utazási idő, a munkavállalót sem terhelő utazási és más költségek, viszonylagos szabadság a munkavégzés során stb.), amelyek hátrányait (pl. munkahelyi közösségek eltűnése) háttérbe szorítják.

Valószínűleg az iskolai, egyetemi oktatás sem kerüli el a sorsát. Nehéz ma még elképzelni a tanulók, hallgatók nélküli oktatási épületeket, a verbális vizsgákat helyettesítő elektronikus üzenetváltásokat stb.

Az e-mail (elektronikus posta) és a BBS (Bulletin Board System - elektronikus hirdetőtábla) program által elektronikus levelek, üzenetek vagy felhívások, információk küldhetők más személynek vagy tehetők "közhírré", bárki által elérhetővé egy helyi telefonhívás áráért röpke pillanat alatt.

2. A SZÁMÍTÓGÉP MEGBOLYGATJA ÉLETÜNKET

Napjaink reálisabb szemléletével tudjuk, hogy a komputerizáció elvitathatatlan jótéteményei mellett együtt kell élnünk valós hátrányaival is.

Növekszik kiszolgáltatottságunk és ezzel együtt félelmünk a különféle számítástechnikai rendszerektől, gondoljunk csak az igazgatási, energetikai vagy honvédelmi rendszerekre.

Még a nyolcvanas évek elején majd száz B-52-es légierődöt riadóztatnak és indítanak az amerikai Stratégiai Légierő Magasabb Parancsnokságának (Strategic Air Command-nek) számítógépei, mert szovjet rakétatámadást jeleznek. Katonai szakértők szerint a kubai rakéta-válság és az afganisztáni bevonulás után ez vol a harmadik világháború kirobbanásának legreálisabb veszélye.[2]

A számítógép működtetése, mint bármely elektronikus készülék az emberi egészségre közvetetten vagy közvetlenül is ártalmas.

Az előbbiek között említhető az ún. compufóbia[3], amely intenzív félelemérzetet, szorongást, neurotikus zavarokat idézhet elő. Másik tipikus panasz az ún. technostressz, amely a számítógéppel nap, mint nap dolgozóknak okozhat közérzeti (pl. nyugtalanságot, levertséget) vagy funkcionális zavarokat (pl. szapora szívműködést, szívdobogást), akár pszichoszomatikus tüneteket (pl. gyomor- és nyombélfekélyt).

Az ún. elektroszmog[4] idézheti elő a tipikus "operátor-betegséget", pl. fejfájást, a szem és a nyálkahártyák kiszáradását, amely viszont további egészségügyi problémák forrása lehet (pl. látásromlás). A számítógép előtt ülők a merev testtartás folytán izom- és ízületi fájdalmakra panaszkodhatnak.

A számítógépek megjelenése, majd elterjedése az egész társadalmat érintő hatásokat hoz magával. A kiszolgáltatottságától való félelem mellett a számítógép szenvedélybetegséget, függőséget is előidézhet. Meglepő, hogy a számítógép "rabjai" némelykor a gépet választják házastársuk helyett. A számítógépek miatti

---

[2] Ralph M. Stair Jr.: Computers in Today's World. Illinois, 1986. p. 502
[3] vö. R. M. Stair p. 515

válásokról számol be a németországi észak-rajna-vesztfáliai Hamm városának Szenvedélybetegségek Központja.[5]

Ha világunk politikai, gazdasági, kulturális és egyéb információbázisai csupán egy-egy forrásból válnak elérhetővé és ezek egy-egy világnyelven olvashatók, akkor jogos az aggódásunk az információ monopolizáltsága és a nemzeti nyelv és kultúra háttérbe szorulása miatt.

Gondolunk-e arra, hogy a számítógép használatával eltűnnek a szerző által írott, javított irodalmi alkotások kéziratai, amelyek tükrözik a mű születésének stációit, "gyötrelmeit", és amelyek az irodalmárok, az irodalombarátok, és a grafológusok számára oly' becsesek.

Persze a komputer okozta társadalmi bonyodalmak közül találhatunk számunkra mosolyt fakasztót, bár az érintettet számára felettébb kellemetlen esetet is. Ez történt 1993. nyarán, amikor az egyesült államokbeli George-Ann Knier és férje 68 037 294 206.- dollár adóhátralék befizetését követelő levelet kapott.[6]

A komputerizáció legszámottevőbb negatív társadalmi hatása azonban a **számítógépes környezetben elkövetett bűncselekmények**. A számítógép akár céljában, akár eszközében részben új típusú bűncselekmények lehetőségét teremti meg. Részben egy-egy hagyományos, több évtizede, évszázada, esetleg még régebben ismert bűncselekmény elkövetésének új, modernebb megvalósulásához járul hozzá. Ez utóbbira utalni fogok az adott bűncselekmények bemutatásánál.

---

[4] vö. R. M. Stair p. 516.
[5] adja hírül a Népszabadság 1995. június 1. 20. lapon
[6] adja hírül az Új Magyarország 1993. július 30. 5.lapon

3. AZ INFORMATIKAI BŰNCSELEKMÉNYEK KRIMINOLÓGIAI ASPEKTUSAI

Az első számítógépes bűncselekmények egyike az egyesült államokbeli Walston end Co. alelnöke által elkövetett sikkasztás, aki - nem kevés fizikai munkával - hamis lyukkártyákat készítve 50.000.- dollárt sikkaszt még a hatvanas évek végén.[7]

Azóta a bűncselekmények *számos fajtáját* ismerjük. Ez a bűnlajstrom a vagyoni haszonszerzéstől, a hamisításon, az adatkikémlelésen, a számítógép, a programok és az adatok ellen véghezvitt erőszakos vagy intellektuális támadáson, a programok és a félvezetők jogosulatlan megszerzésén, másolásán, kereskedésén át a bankkártyákkal történő visszaélésekig terjed.

A technika fejlődésével feltűnnek a legmodernebb jogsértések; a mobiltelefonokhoz tartozó SIM-kártya manipulálása, valamint az intra-, extra- és Interneten elkövethető, azokon megjeleníthető jogellenes cselekmények formájában.

A számítógépes környezetben elkövetett deliktumok - a fizikai rongálást kivéve - zömében *intellektuális* cselekmények. A számítógép, és a hozzá kapcsolódó technikai eszközök kezelése komoly felkészültséget, fantáziát, nem csekély logikai készséget követel. A vagyoni kárt okozó jogsértések is igazi intellektust igényelnek, pl. a vírusok, "férgek", "logikai bombák" létrehozása, és azok számítógépes rendszerekbe juttatása.

A számítógéppel elkövetett bűncselekmények - a kriminológia kategóriáit alapul véve - a *fehér - galléros bűnözés* (white - collar crime) része, bár azt nem fedi le teljesen.

Az üzletemberek bűnözéséről először **Emile Durkheim** francia szociológus, a "szociológia atyja" ír 1902-ben. Következtetése az, hogy "legelítélendőbb

---

[7] Roy Freed: Computer Fraud - A Management Trap Business Horizons 1969. June p(s). 23-28.

cselekményüket gyakran a siker mentesíti a következményektől", emiatt elmarad felelősségre vonásuk. [8]

E. A. Ross egyesült államokbeli szociológus 1907-ben "criminaloid"-nak nevezi azokat a prominens üzletembereket, akik becsapják a fogyasztókat, de megmenekülnek a számonkérés alól, mivel tevékenységük a hatályos törvény szerint nem minősül bűncselekménynek. [9]

Mint köztudott a fehér - galléros bűnözés fogalmát először **Edwin Sutherland** szintén egyesült államokbeli kriminológus definiálja a fehér - galléros bűnözés fogalmát egy 1940-ben kiadott tanulmányában. Ezt a kifejezést használja a felsőbb osztályok (upper class) bűnözésének jellemzésére, szembeállítva azt az alsóbb osztályok (lower class) bűnözésével.

Sutherland 1949-ben már precízebb fogalom-meghatározást nyújt, e szerint fehér - galléros bűnöző az, aki a bűncselekményt tekintélyének és magas társadalmi státuszának felhasználásával, munkája folyamán követi el. [10]

A későbbiekben a kriminológusok egységesen elfogadott értelmezés hiányában gazdasági, szervezeti, illetve foglalkozási bűnözésnek is tekintik a fehér - galléros bűnözést.

Az egyesült államokbeli **Ramsey Clark**, aki kriminológiát oktat a texasi és chicagoi egyetemen, majd ügyészként dolgozik tapasztalatai alapján úgy véli, hogy valamennyi bűnözési forma közül fehér - galléros bűnözés a legrombolóbb, mivel az e körbe vonható bűncselekmények elkövetői hivatali - hatalmi helyzetüket felhasználva fosztanak meg másokat vagyoni javaiktól. Erkölcsi megítélésük ezért lényegesen kedvezőtlenebb, mint más bűncselekmények esetében. A szerző szerint az áldozatok számára a következmények súlyosabbak, mert "sokkal mélyebbre tud ásni a zsebben levő pénztárcánál, mivel elvonja egy élet megtakarításait."[11]

---

[8] Émile Durkheim: The Division of Labor in Society. New York, 1964. p. 2.
[9] Edward Ross: The Criminaloid. The Atlantic Monthly, 1907. 4. p. 45.
[10] Handbook of Criminology (Editor: Daniel Glaser.) Chicago, 1974. p. 283.
[11] Ramsey Clark: Crime in America. New York, 1971. p. 23.

A fehér - galléros bűnözésen belül a szakirodalom foglalkozási (occupational) és szervezeti (corporate) bűnözés között különböztet.[12] Ennek alapja - a cselekvések örök mozgatója, vagyis - az elkövető ténykedése cui prodest.

Foglalkozási bűncselekményről beszélünk abban az esetben, amikor az elkövető munkakörét felhasználva saját magának szerez jogtalan előnyt, vagyoni hasznot. A magyar büntető törvénykönyvben lapozgatva fellelhetjük a sikkasztást (Btk. 327. §), a bennfentes értékpapír-kereskedelmet (Btk. 299/A. §), a passzív vesztegetést (Btk. 252. §) stb. A számítógépes környezetben az azzal dolgozó alkalmazottak mellett az operátorok, a számítógép-kezelők a tipikus elkövetők.

Szervezeti bűncselekményeket a szervezet érdekében, a szervezet számára biztosítandó előny, vagyoni haszon eléréséért követnek el. E körbe sorolhatók az alábbi nálunk kriminalizált bűncselekmények: adó-, társadalombiztosítási csalás (Btk. 310. §), munkanélküliek szolidaritási alapjába fizetendő munkaadói és munkavállalói járulék fizetési kötelezettség megszegése (Btk. 310/A. §), a társadalombiztosítási, egészségbiztosítási vagy nyugdíjjárulék fizetési kötelezettség megsértése (Btk. 310/B. §), a hitelsértés (Btk. 330. §), a tartozás fedezetének elvonása (Btk. 330/A. §) vagy akár az üzleti titok megszerzése a konkurens cégtől (Btk. 222. §) stb.

E rövid áttekintést követően megállapíthatjuk, hogy a számítógéppel elkövetett bűncselekmények a fehér - galléros bűnözés mindkét most vázolt csoportjára jellemzőek lehetnek. Azonban e körön túl is mutathatnak, hiszen a számítástechnikai rendszerekbe történő jogtalan behatolás, különféle jogosulatlan műveletek végzése, titkok kifürkészése, kívülálló (extraneus) által elkövetett jogsértések vagy e rendszerek elleni terrortámadások nem vonhatók ide. Egyetértek **Balogh Zsolt György** következtetésével, aki leszögezi, hogy "mind a számítógépes, mind a fehér-galléros bűnözés olyan önálló kriminológiai kategória, melyek között van ugyan némi átfedés, de arról mégsincs szó, hogy bármelyik kategória egészében tartalmazná a másikat." [13]

---

[12] William J.Chambliss: Exploring Criminology. New York, 1988. p. 63
[13] Balogh Zsolt György: Jogi informatika. Budapest-Pécs, 1998. 266.l.

A fehér - galléros bűncselekmények nyomozását éppen az a szociológiai körülmény nehezíti, hogy az elkövetők általában büntetlen előéletűek, a hatóságok "a priori" bizalommal viseltetnek e személyekkel szemben és nem utolsó sorban jogi védelmüket körültekintőbben, hatékonyabban szervezhetik meg másoknál.

Mivel minden kriminálétiológia kutatás a kriminalprofilaxist szolgálja, így a számítógépes környezetben elkövetett jogsértések *motívumainak* megismerése elsődlegesen nemcsak a nyomozati cselekmények eredményességét segíti, hanem a bűnmegelőzés lehetőségét is erősíti. Az informatikai bűncselekmények motívumai rendkívül változatos képet mutatnak. A kriminológiai kutatások tapasztalatai azt jelzik, hogy a számítógépet új, modern eszközt *először* jogosulatlan vagyoni haszonszerzés céljából használják fel a "high-tech" bűnözők. Egy a nyolcvanas évek elejéről származó FBI - jelentés kiemeli, hogy míg a fegyveres bankrablással az elkövetők átlag tízezer dollárt zsákmányolnak, addig a komputeres elkövetés révén átlag egy millió dollárt.[14] Ha a számok szükségszerűen változnak az azóta eltelt időben, az a tendencia nem kérdőjelezhető meg, hogy e korszerű eszközzel lényegesen *jelentősebb vagyoni kár okozható*, mint hagyományos, fegyveres bankrablással. Ne felejtsük el azt sem, hogy amíg egy-egy pénzintézet falai, mint egy erőd emelkednek a bűnelkövetők előtt (pl. a londoni Bank of England épülete), továbbá a rablóknak számolni kell a bank biztonsági embereinek fegyveres ellenállásával, addig a helyszíntől akár több száz (vagy ezer) kilométer távolságból indított számítógépes betörés elkövetéséhez elegendő egy komputer, egy hozzákapcsolódó modem és egy ahhoz kapcsoló telefon. Ne feledjük azt sem, hogy az "elektronikus betörő" élete sem kerül veszélybe. Nem kell fegyverrel és atletikus képességekkel rendelkeznie, és a menekülését, gyanús útlezárásokkal, színlelt balesetekkel biztosítani stb.

Mind ez ideig a legtetemesebb kárt okozó bűncselekmény-sorozatot, - amelyről a Guiness Rekordok könyve is megemlékezik - 1963-74 között követik el, amikor is az *Equity Funding Corporation* (egyesült államokbeli biztosító társaság)

---

[14] W.H. Cunningham - R. Aldag - C.M. Swift: Introduction to Business. Cincinatti, Ohio 1984. p. 445.

számítógépeivel a cég munkatársai hamis kötvényeket készítenek, amelyekre fiktív kifizetéseket eszközölnek. Hatvannégyezer fiktív biztosítási káresetért kettő millió dollárt fizettetnek ki a társasággal.[15]

Az egyedi tettesi "kategóriában" egy *Stanley Mark Rifkin* nevű fiatalember viszi el az igencsak kétes értékű pálmát. 1980-ban, elítélésekor is csak 34 éves. Számítástechnikai tanácsadóként dolgozik a los angelesi Securtiy Pacific bankban. Itt az alkalmazottak az aznapi forgalmat az ügyfelek kódjaival egymásnak átkiabálják. Rifkin 1978 október 25-én egy utcai telefonfülkéből egy ügyfél számlaszámról (736.) a hozzárendelt kódszám (54739.) azonosításával 10,2 millió dollárt utaltat át a new yorki Serving Trust Bankba. A bűncselekményt 8 nappal később észlelik, majd később a telefonhívás alapján azonosítják a telefonáló nevét. Közben Rifkin az átutalt pénzből Svájcban egy fiktiv cég (Rusalmaz) nevében gyémántot vásárol. Visszatérvén az Egyesült Államokba ügyvédjének könnyelműen kérkedik gyémántjaival, aki azonban feljelenti. A bíróság az elkövető cselekményét lopásnak minősítve 9 évi szabadságvesztés büntetést szabott ki.[16]

Ez az eset jellemzően példázza e bűncselekményfajta kriminológiai jellemzőit: a leggyengébb láncszem a védelmi rendszerben maga az ember. A bűncselekmény megvalósítója magasan kvalifikált, a számítástechnikában jártas személy.

A számítógépes hálózatok világméretűvé válásával *bármely ország állampolgára, bármely időpontban, bármilyen távolságra levő pénzintézet, hivatal vagy más intézmény* adatállományához hozzáférhet. Az idegen elektronikus adatfeldolgozó rendszerekbe történő jogtalan behatolást és az ott tárolt, más előtt védett adatok megszerzése a *hacking*. A hackerek azok, akik a legkülönfélébb motívumoktól indíttatva lépnek be idegen számítógépbe vagy hálózatokba. A hacker olyan mesterember, aki faipari munkát végez, fát farag stb. Az 50-es évek

---

[15] A.N. Smith - W.J. Alexander - D.B. Medley: Advanced Office Systems. Cincinatti, Ohio 1986. p. 402.
[16] vö. R.M. Stair p. 505

végén az MIT nagygépek programozói nevezik magukat így. Az akkori nagygépek szűk memóriakapacitásával küszködnek. A programokból törekszenek "faragni", hogy minél több hely maradjon a feldolgozni kívánt adatok számára. Itt gyökerezik a 2000. év számítástechnikai problémája az ún. Y2K-probléma (a "milleneumi bomba"). A 2000-et takarékossági megfontolásból 00-nak ábrázolták. Ezáltal az évszám a számítógép számára 1900-zal vagy más 00-ra végződő évszámmal összekeverhető. A probléma feloldására pótlólagosan programokat készítenek, amely a szoftveriparnak jól jövedelmező üzlet, biztos piac. Bár vitathatatlan veszélyt rejt egy - egy számítógépes rendszer (energia-, pénzügyi stb.) leállása.

A hackerek később szellemi kihívásként, "párbajként" fogják fel a számítógépet vagy a rendszereket védő kódok megfejtését, vonzza őket a kíváncsiság, az unalom, a játékosság vagy a társak előtti dicsekvés vágy. Ma már az "elektronikus betörők" igazi profik - talán a hajdani "hackerek nagy generációja" - akik gyakorta a szervezett bűnözés szolgálatába szegődve, megbízásból pénzért, kábítószerért, fanatista hitükért aprózzák el tudásukat.

A "hacking" veszélyére a nyolcvanas évek közepén figyelnek fel, amikor hamburgi, hannoveri és az akkori nyugat-berlini fiatalok a KGB felbujtására az akkori kelet-berlini szovjet kereskedelmi kirendeltség kommunikációs hálózatát használva a Lawrence Berkley Laboratórium vonalán keresztül a Pentagon (az amerikai Védelmi Minisztérium), a NASA (az amerikai Légügyi és Űrhajózási Hivatal), a los alamosi nukleáris laboratórium és más katonailag fontos intézmények számítógépeinek adatállományaihoz férkőztek hozzá. A nyugat-német bíróság 1990. február 15-én kelt ítéletében az elkövetőket kémkedésért kettő évet el nem érő szabadságvesztéssel sújtják. [17]

Az USA kormányzat 1999. tavaszán a NATO Jugoszlávia ellen vívott háborúja ideje alatt olyan hackereket keres, akiknek az akkori jugoszláv elnök,

---

[17] Dr. Ulrich Sieber: A számítógépes bűnözés és más bűncselekmények az információtechnológia területén. MJ. 1993. 2.sz. 105-109.l., valamint,
a Revue Internationale de Droit Penal 1993/1-2. p. 326., és
Dr. Wolfgang Bär: Der Zugriff auf Computerdaten im Strafverfahren. Köln* Berlin * Bonn * München, 1992. s. 37.

Milosevics feltételezett görögországi, ciprusi, oroszországi bankszámláihoz kellett volna hozzáférniük és azokról a pénzösszegeket lehívni, ezáltal akadályozandó meg szökését.[18]

A leghíresebb-hírhedtebb hacker *Kevin Mitnick (*alvilági nevén Condor), aki az ezredfordulón 35 éves, de már többször elítélik a legkülönfélébb elektronikai bűncselekményekért. 1988-ban egy évi szabadságvesztésre ítélik program másolásért, bankkártyák számainak megismeréséért. Szabadulása után továbbra is illegálisan „látogatja" a több tucat telefontársaság, szoftvergyártó cég hálózatát, ahonnan mobiltelefonok kódjait, szoftvereket szerez. 46 hónapi szabadságvesztésre ítélik. Három évre eltiltják számítógép, mobiltelefon és egyéb technikai eszközök használatától.[19] A szintén egyesült államokbeli *Kevin Poulsen*, betörve egy telefoncég hálózatába a nyereményjáték rendszerét úgy alakítja át, hogy a sorsoláson egy autó „szerencsés" nyertese lesz.[20]

A szervezett bűnözők is fantáziát látnak az elektronikus betörés nyújtotta lehetőségekben. Az orosz maffia megbízásából *Vladimir Levin* 1994-ben Szentpétervárról negyven alkalommal több mint tíz millió dollárt hív le az egyesült államokbeli Citibank számláiról és a pénzösszegeket holland, finn stb. bankok számláin helyezi el. Angliába érkezésekor tartóztatják le és az eljárás az USA-ban mind a mai napig tart.[21]

Az Interneten barangolva sokféle „cyberblotter", azaz „körözési felhívás" olvasható a legveszélyesebb hackerekről.[22]

Nem kevésbé kísérteties, sőt hátborzongató az egyesült államokbeli milwaukee-i "414-esek" (az ottani körzet hívószáma) esete. Az elkövetők manhattani Sloane-Kettering Memorial Cancer Center számítógépes rendszerébe

---

[18] adja hírül a Newsweek CXXXIII. No.22. May 31. 1999. p. 22.
[19] adja hírül a http://index.hu/cikkek0001/kevinm, valamint
a http://www.usdoj.gov/usao/cac/pr/cac70627.1.html, és
a http://www.comm.fsu.edu/com4330/summer/essay/lrp2.htm
[20] adja hírül a http://www.discovery.com/area/technology/hackers/hackers.html
[21] adja hírül a http://www.itd.nrl.navy.mil/ITD/5540/i...ms/old-news-items/950918.Citibank.html
[22] adja hírül a http://uainfo.arizona.edu/~weisband/411_511/cyberblotter.html

hatolnak be és átprogramozzák az ott kezelt rákbetegek adatait. A csoport egyik 17 éves tagja fedi fel a sajtónak cselekedetüket.[23]

A "hacking" motívumait színesíti azoknak a san diegoi (USA) diákoknak a leleménye, akik ily módon javítják ki iskolai osztályzataikat.[24]

A lengyel **Andrzej Adamski** felveti a "jó hacker" gondolatát.[25] Nem kétséges, hogy tevékenykednek olyan jó szándékú hackerek, akik letörlik a pedofil és más pornó oldalakat, a gyűlöletkeltésére alkalmas uszításokat, a kábítószer-fogyasztást népszerűsítő -, a bombakészítést bemutató oldalakat, a valóságos háborút kísérő cyber - háború propagandáját, a levelezési listákat elárasztó reklámokat stb. Ugyanakkor bármennyire nemes szándék is vezérli a "jó hackert", ő valamely védett rendszerbe lép be jogosulatlanul és ezzel kárt okoz a helyi hálózat üzemeltetőjének. Magatartása emlékeztet az önbíráskodásra, ami jogilag tilalmazott.

Valószínűleg igen naiv az a gondolatom, hogy a hackerek szaktudását talán a társadalom javára is lehetne forgatni, korunk vezéreszméjét szem előtt tartva természetesen honorárium, vagy "vádalku" fejében.

További kriminológiai sajátosság a bűncselekmény elkövetésének *időzítése*, amely szintén a felderítést nehezíti.

A számítógéppel elkövetett bűncselekmények további lényeges jellemzője az elkövetés hihetetlen *gyorsasága.* A másodperc tört része alatt - megközelítőleg ennyi időt vesz igénybe egy billentyű lenyomása - olyan adatok törölhetők, kiegészíthetők, felülírhatók azaz módosíthatók vagy megismerhetők, lehívhatók, amelyek vagyon értéket jelző vagy bizonyító erejű adatállományok jelentékeny mértékben károsodhatnak, értelmük, értelmezhetőségük és értékük ezzel megváltozhat, titkosságuk törést szenvedhet. Az elkövetés gyorsasága a

---

[23] vö. A.N. Smith - W.J. Alexander - D.B. Medley p. 402.
[24] vö. R.M. Stair p. 508.
[25] Dr. Andrzej Adamski: Crimes related to Computer Network. ("Bűncselekmények a számítógépes hálózattal összefüggésben") c. előadásának szövegéből 20-22.l. kéziratban.

bűncselekmény veszélyességét növeli, mivel a tettenérés nehézkessége gyengíti az eredményes nyomozást, ezáltal a büntetőjogi felelősségrevonást végső soron a bűnmegelőzés esélyeit.

A rendelkezésre álló *német bűnügyi rendőrség statisztikai adatai* a kilencvenes években azt mutatják, hogy a számítógépes és a bankkártya csalás ezres nagyságrendűek (1990-ben észlelt számítógépes csalás 787, bankkártya csalás 3963, illetőleg ugyanezen adatok 1991-ben 1035 és 5701). A többi számítógéppel elkövetett bűncselekmények száma százas nagyságrendűek (az elemzett időszakban az adatváltoztatás és más szabotázs cselekmények száma 95 és 135, komputerrel végrehajtott hamisítások száma 82 és 106).[26]

A német statisztikai adatok azt jelzi, hogy a számítógéppel elkövetett bűncselekmények az összbűncselekmények töredéke. De okkal - joggal gyanakodhatunk magas látenciára is.

Magyarországon 1994-ben még csak egy számítógépes csalás válik ismertté, ám számuk 1998-ra 368. A kárérték 1995-ben 1 534 800.- forint, ám 1998-ban 219 994 400.- forint.[27]

A bűncselekmények számával összefüggésben nyugodtan kijelenthetjük, hogy e körben nagyfokú *látenciájával* kell számolnunk. Az ismertté váló bűncselekmények minden bizonnyal csupán a "jéghegy csúcsa". Nem véletlenül nevezi az e tárgyban elsőként napvilágot látott ENSZ - tanulmány a számítógéppel elkövetett bűncselekmények egy részét **Hans von Hentig** kriminológus elnevezése után az összbűnözés "sötét mezőjének".[28] Megjegyzem, hogy ehelyütt a látencia tágabb értelmezése kerül előtérbe, vagyis azon jogsértő cselekményekről is szó van, amelyek nem jutnak a hatóság tudomására.[29]

Az előadás elhangzott a "VI. European Colloquium on Crime and Criminal Policy, Helsinki 1998. december 10-12-én

[26] Revue ..... p(s). 322 -323.

[27] adja hírül a Népszabadság, 1999. november 27 az 5. lapon

[28] Draft United Nations Manual on Computer - Related Crime (kézirat). (Készült a Kanadai Igazságügyminisztériumban, Ottawa, 1992.) p. 9.

[29] Dr. Korinek László: Rejtett bűnözés. Budapest. 1988. 16.l.

A látencia okai közt említhetjük azt, hogy a jogsértéssel előidézett kár általában eltörpül a károsult szervezetek, intézmények, cégek (bankok, biztosítók, vállalatok) jó hírnevében (goodwill-jében) bekövetkezhető hátrányokhoz képest. Hiszen érthető bizalmatlanságot válthat ki az ügyfelekben, ha kitudódik hogy valamely pénzintézet számítástechnikai rendszere sebezhető, oda könnyedén be lehet jutni, a számlákról pénzt lehet leemelni, átutaltatni avagy az ott tárolt személyes adatokhoz hozzá lehet férni. Ezen intézmények ellenérdekeltek a nyomozó hatóságok törekvéseivel.

További oka a látenciának, hogy a lelepleződés szinte véletlenszerű. Nem egyszer a kárt szenvedett intézmény, szervezet szakértelméért alkalmazta a leleplezett jogsértőt.

Ugyanakkor túl is becsülhetjük a felderítetlen cselekmények számát, amelynek okai az alábbiak lehetnek:

- a sajtó a korábbi években az egyes számítógépes visszaélésekről (pl. a milliós csalásokról vagy számítógépes a vírusokról) szenzációként számol be olvasóinak. Ez sugallja a cselekmények veszélyességét.
- Aki nem dolgozik számítógéppel, az óvakodik, sőt fél ettől a modern technikai vívmánytól. Számukra ezért hihetőek e "szenzációk".
- Az érzékeny számítástechnikai rendszereket (energetikai, honvédelmi, államigazgatási stb.) több rendkívül komoly potenciális veszély fenyegeti. Viszont ennek bekövetkezése igen csekély vagy soha be sem következik.
- Nem szabad lebecsülni azoknak a jól felkészült, lelkiismeretes számítástechnikai szakemberek munkáját, akik a számítógépes rendszerek minél teljesebb körű védelmére, biztonságára törekszenek.

4. A BÜNTETŐPOLITIKÁT ÉS A BÜNTETŐ-JOGTUDOMÁNYT ÉRŐ KIHÍVÁS

Az *1960-as évek*ben a számítógépes környezetben megjelent bűncselekményeket először, mint a fantasztikus irodalomba vagy a mesék világába tartozónak említik, lényegében kuriózumnak vélik. Később is mindössze a tradicionális bűncselekmények új modus operandijának tekintik. [30]

Az *1970-es évek*ben elején megjelennek az első tanulmányok, amelyek az új típusú cselekményeket elemzik, és a büntetőjogi értékelés lehetőségeit vizsgálják. Az első elemzések nagyjából négyféle bűncselekményfajtát különböztetnek meg: számítógépes visszaélést, a számítógépes szabotázst, a számítógépes kémkedést, és a gépidő-lopást. Az évtized második felének tendenciája a technika gyors fejlődésével a nagy tömegű adatfeldolgozás igénye. Ez felszínre hozza azon veszélyeket, amelyekkel az érintett személyek számolhatnak. Ezzel együtt fontos politikai célként fogalmazzák meg az állami szervek működéséről, a költségvetés helyzetéről, a környezetvédelemről és minden az állampolgárokat érdeklő és érintő közérdekű információk megismerésének az igényét.

Az egyre bővülő elektronikus adatfeldolgozás egyre bonyolultabb programokat igényel. Fellendül a szoftvergyártás ipara.

Az elektronikus adatfeldolgozás tehát *új értéket, érdeket* teremt: ezek a testetlen, láthatatlan elektronikus impulzusok, azaz olyan adatok, amelyek információt hordoznak és olyan adatok, amelyek egy-egy program építőkockái.

Az *1980-as évek*ben az elektronikus adatfeldolgozás elterjedésével a jogsértő magatartások elszaporodása, további új típusú visszaélések felszínre kerülése az országokat arra ösztönözte, hogy a büntetőjog eszközeihez nyúljon. Ehhez ad támpontot az évtized közepén napvilágot látó OECD-jelentés (1986.), majd az

---

[30] Dr. Ulrich Sieber: The International Emergence of Criminal Information Law. Köln * Berlin * Bonn * München, 1992. p.3.

évtized végén az Európa Tanács által kibocsátandó Ajánlás (1989.). Mindkettő a bűncselekmények osztályozásáról, ezek meghatározásáról szól.

Kezdetét veszi ezen cselekmények kriminalizálása szerte a világon. Tipikusan új tényállásként kerülnek be a büntető törvénykönyvekbe a számítógépes csalás és az adatvédelemmel összefüggő tényállások. Megerősítést nyer a szerzői jog büntetőjogi védelme.

Az *1990-es évek* felszínre hozzák az összbűnözésen belül szignifikánssá váló bűncselekmények nyomozásával összefüggő aggályokkal. A jogalkalmazás során felvetett problémák megoldására tesz számos javaslatot az Európa Tanács Ajánlása (1995.).

Az évtized kiemelkedő produktuma az Internet, amely földrészeket összekötve, a leggyorsabb adatátviteli módon egyelőre jogi kötöttségek nélkül tág teret nyit az információáramlásnak és ezzel a jogsértéseknek is.

Magyarországnak is fel kell készülnie az elektronikus adatfeldolgozás folyamatában, - annak befolyásolásával vagy felhasználásával - véghez vihető jogsértések kriminalizálására, e bűncselekmények nyomozásához szükséges új rendelkezések kidolgozására.

A büntetőjogi beavatkozás körének, mértékének meghatározása a mindenkori kormány *büntetőpolitikájának* hatókörébe tartozik.

Finkey Ferenc már századunk első évtizedeiben úgy vélte, hogy a "bűnügyi politika ..... a bűnelkövetés tényezőinek megszüntetését vagy legalább ellensúlyozását, ezzel a bűntettek csökkentését, az erre szolgáló módozatok, reformintézmények és intézkedések megvitatását és kiépítését tekinti feladatának." [31]

Napjainkban a bűnügyi politika megnevezés helyébe lépett a kriminálpolitika vagy büntetőpolitika. Ez a kettősség egyes szerzőknél némi tartalmi eltérést is tükröz. **Pusztai László** szerint a kriminálpolitika tágabb kört ölel fel, mint a

---

[31] . Dr. Finkey Ferenc: A magyar büntetőjog tankönyve. Budapest, 1914. 48.l.

büntetőpolitika, mivel az előbbinek például figyelmet kell fordítania a büntetőjogi útról történő eltereléssel összefüggő problémákkal is.[32]

Ezzel szemben **Földvári Józseffel** együtt magam is a kriminálpolitika érvényesülési körét a kutatás egzaktsága, behatárolhatósága végett a büntető jogalkotásra és jogalkalmazásra korlátozom.[33] Ez utóbbi azonban nem szűkíthető le a bíróságok munkájára, hanem kiterjed a bűnüldözésre és a büntetés-végrehajtásra is.

A kriminálpolitikai döntések hatása túlnő az igazságszolgáltatás keretein, ahogy ezt **Farkas Ákos** konstatálja, "amióta a büntető igazságszolgáltatás és a bűnmegelőzés egyre szorosabb vonatkozásba kerültek egymással, illetve bizonyos igazságszolgáltatási feladatok a bűnmegelőzés körébe kerültek át, a kriminálpolitika erre a területre is kifejti hatását." [34]

A kriminálpolitika a kormány általános politikájának része, azzal adekvátan - "rendszerezi, rangsorolja, fogalmazza meg azokat a prioritásokat, melyek jogalkotási tárgyakká, illetve konkrét jogszabályokká válnak."[35]

A büntető-jogtudomány zárt ismeret- és fogalmi rendszere, belső összefüggései, törvényszerűségei azok a szűrők, amelyek jogi keretek közé kényszerítik a büntetőpolitikai elképzeléseket, kívánságokat.

Az állami büntetőpolitika egyszerre tudomány és gyakorlat. Tudomány **Földvári József** megfogalmazásában, mivel a büntetőpolitika azon "ismereteknek a rendszere, amelyek alapján szervezheti az államhatalom a bűnözés elleni küzdelmet,

---

[32] Interjú Dr. Pusztai Lászlóval "A bűnözésről, a büntetőpolitikáról ....." Rendészeti Szemle XXXI. évf. 5. sz. 1993. május 49-50.l.

[33] Dr. Földvári József: Kriminálpolitika. Budapest, 1987. 21.l.

[34] Dr. Farkas Ákos: A bűnözés okozta válság - a jogállami büntető igazságszolgáltatása válsága. Ünnepi tanulmányok II. Horváth Tibor 70. születésnapjára. (Szerkesztette: Farkas Ákos, Görgényi Ilona, Lévai Mikós.) Miskolc, 1997. 195.l.

[35] Dr. Farkas Ákos: A kriminálpolitika és a büntető igazságszolgáltatás hatékonysága. Tanulmányok Szabó András 70. születésnapjára. (Szerkesztette: Gönczöl Katalin és Kerezsi Klára.) Budapest 1998. 85.l.

meghatározván e küzdelem eszközeit, ezen eszközök alkalmazásának feltételeit és módjait, összhangban az általános politikai célkitűzésekkel."[36]

A büntetőpolitika gyakorlat is egyben, amelynek során az állam különböző formális és remélhetően minél szűkebb körben, - a demokrácia fokától, a társadalmi kontroll fejlettségétől függően - informális befolyásával próbálja érvényre juttatni elképzeléseit a jogalkalmazás terén. A kriminálpolitika egységes rendszerében a tudomány és gyakorlat kettőssége egyszerre és egymást kiegészítve jelenik meg és hat.

E két elem kívánatos összhangja nem mindig teljesül. Előfordulhat a büntetőpolitikai elképzeléseket jogszabályi formába öntő jogalkotást nem követi a jogalkalmazás személyi, anyagi feltételeinek biztosítása. Vagy a jogalkalmazás nem tud funkciójának megfelelni a jogalkotás hiányosságai, következetlensége miatt.

Ha a büntetőpolitikát a büntető törvényhozásra szűkítjük, mint ahogy **Wiener A. Imre** megállapítja, akkor a "büntetőpolitika egyrészt vélemény arról, hogy mi legyen bűncselekmény, mit kell büntetendővé nyilvánítani, másrészt arról, hogy ennek a cselekménynek milyen súlya van, milyen mértékben kell büntetni."[37]

E meghatározáshoz **Békés Imre** hozzáteszi, hogy a "büntetőjog alkotásában mindig az adott kor és azon belül az adott történelmi időszak politikai - gazdasági - társadalmi igényei érvényesülnek; a büntetőjog ezeknek az igényeknek nem létrehozója, hanem csak szolgálója."[38]

A büntető-törvényhozás koncepciója **Földvári József** szerint a szabályozás szükségességéből és hasznosságából fakad. [39]

A szabályozás *szükségessége* annak felismerése, hogy milyen magatartások kriminalizálásával érhető el a társadalmi együttélés rendje, nyugalma. Míg a

---

[36] Dr. Földvári József: Kriminálpolitika .... id. mű 22.l.
[37] Dr. Wiener A. Imre: Büntetőpolitika - büntetőjog (jogszabálytan) ("Büntetendőség - büntethetőség" c. tanulmánykötet. Szerkesztette: Dr. Wiener A. Imre) Jog és jogtudomány 13. Budapest, 1997. 11.l.
[38] Dr. Békés Imre - Dr. Földvári József - Dr. Gáspár Gyula -Dr. Tokaji Géza: A magyar büntetőjog általános része. Budapest, 1980. 11 - 12.l.
[39] Dr. Földvári József: Kriminálpolitika id. mű ..... 68 - 72.l.

szabályozás *hasznossága* a társadalom tagjai viselkedésének pozitív befolyásolásában mutatkozik meg.

A büntetőjog funkciójának adódóan a kormányzat politikai indíttatásból, átgondolatlan büntetőpolitikai törekvések miatt, szimpátia- vagy valódi voksok szerzése végett elhamarkodottan nyúl(hat) a büntetőjog kemény eszközeihez. Ezzel összefüggésben **Nagy Ferenc** "vissza-visszatérő tévhit"-ként jellemzi azt az egysíkú felfogást, amely szerint "a büntetőjogi szabály meghozatala, főként annak szigorítása a nem kívánatos társadalmi jelenségek, a bűnelkövetések megszüntetéséhez illetve visszaszorításához önmagában vagy nagyrészt elegendőek és ez nyújtja a megfelelő megoldást, a gyógyírt."[40]

A reális kriminálpolitika követelményét **Finszter Géza** úgy summázza, hogy "a jó kormányzás maga kompetenciáját elsősorban a pozitív kontrollmechanizmusok kialakításában határozza meg. (Szociálpolitika, egészségügy, oktatás, kultúra, környezetvédelem.)"[41]

A kriminálpolitika hatékonyságáról **Lévai Miklós** azt állapítja meg, hogy "a (büntető)politika hatékonyságát a döntésekkel érintett szférák racionalitásainak egyeztetése biztosítja."[42]

Bizton állítható, **szakmánk azon meggyőződése**, hogy a bűnözéssel szembeni küzdelemben e kriminálpolitikán kívül eső területek pozitív irányú befolyásolása, fejlesztése bír prioritással.

Nem kétséges, hogy ez a legnehezebb, legkockázatosabb és legköltségesebb feladat. Az sem szabad, hogy hitünket megtörje, ha ez kecsegtet a legkevesebb sikerrel.

A büntetőjog a jogrendszer represszív jogágai között a legszigorúbb és ez tény körültekintésre kell, hogy intse a törvényhozót. **Merényi Kálmán** felhívja a

---

[40] Dr. Nagy Ferenc: Változási tendenciák és ellentmondások a büntetőjogban. Ünnepi tanulmányok II. Horváth Tibor 70. születésnapjára. (Szerkesztette: Farkas Ákos, Görgényi Ilona, Lévai Miklós.) Miskolc, 1997. 81-82.l.

[41] Dr. Finszter Géza: Európai rendészeti modellek és a magyar rendőrség. Kriminológiai Közlemények 57. Budapest, 1999. 241.l.

figyelmet ennek következményire, "a büntetőjog alkalmazását csak végső esetben, más módszerek sikertelensége esetén "ultima ratioként" lehet igénybe venni, de ez mindig kockázatos, egyaránt sértheti a társadalom érdekeit és durván beavatkozhat az egyének legszorosabban vett magánéleti, intim szférájába."[43] A szerző előbbi gondolatával összefüggésben már most jelezzük azt a dilemmát, amely a szerzői jog büntetőjogi védelme kapcsán felmerül. A számítógépes szoftver büntetőjogi védelme napjainkban túlkriminalizált. A szerző utóbbi megállapításához kapcsolódva nem egyszerű feladat az információ szabad áramlásának követelményének elvét összhangba hozni, optimalizálni a személyes adatok védelmének elvével. Az egyén intim szféráit érzékenyen érinti az adat- és a magántitok védelmére szolgáló szabályainak kialakítása.

A nemzeti büntetőpolitika kialakítását mind erőteljesebben és szükségszerűen befolyásolja a *nemzetközi jogfejlődés*. A világ anyagi - termelési, műszaki - technikai összekapcsolódása az alapja a nemzeti jogok, így a büntetőjog közelítésének. Ez utóbbi objektív folyamatot erősíti egy másik, objektív jelenség, a nemzetközivé váló bűnözés. Mindezen tényezők a bűnügyi együttműködés elmélyüléséhez vezetnek.

Hazánk visszatérése Európa fejlett, demokratikus országai közé megköveteli, hogy elfogadjuk, a belső jog részévé tegyük azon nemzetközi normákat, amelyeket ezen országok is elismernek, követnek.

A magyar anyagi és alaki büntetőjogban elsősorban az alapelvek közé került, de a tételesjog szabályai közé is bekerültek a Polgári és Politikai Jogok Nemzetközi Egyezségokmányának, az Európai Emberi Jogi Konvenciónak, a Szociális Chartának és más normáknak, valamint az Emberi Jogi Bíróság határozatainak rendelkezései. Ezek egyfelől *előírják* egyes cselekmények (pl. a béke, az emberiség

---

[42] Dr. Lévai Miklós: Kábítószerek és bűnözés. Budapest, 1992. 198.l.

[43] Dr. Merényi Kálmán: Gondolatok a nemi erkölcs elleni bűncselekmények közelmúltbeli változásáról.
Tanulmányok Szabó András 70. születésnapjára. (Szerkesztette: Gönczöl Katalin és Kerezsi Klára.) Budapest,
1998. 176.l.

elleni bűncselekmények, a terrorcselekmény, a kábítószerrel összefüggő magatartások) kriminalizálását, illetőleg a kötelezően alkalmazandó büntető-eljárási (az őrizet időtartama stb.) vagy büntetés-végrehajtási (pl. egy elítéltre eső légköbméter) szabályokat. Másfelől *megtiltják* egyes cselekmények üldözhetőségét, vagy egyes szankciók (pl. a halálbüntetés) alkalmazhatóságát.

Az informatikai bűncselekményekre vonatkozó EU iránymutatás még nincs. Az Európa Tanácsnak már kibocsátott két Ajánlást e tárgykörben:

- az 1989-ben kiadott (9. sz.) "Bűncselekmények számítógépes környezetben" címmel, és
- az 1995-ben napvilágot látott (13. sz.) "Büntetőeljárásjogi problémák az információtechnológiai bűncselekmény körében".

Az előbbi dokumentumban az ET. kialakít egy ún. minimum és egy másik ún. opciós listát, amelyek kriminalizálni javasolt cselekményeket definiálják. Az utóbbi Ajánlás a büntető eljárás során, kiváltképp a nyomozás teljesítésekor ismertté vált problémák feloldására tesz javaslatot. Ezen "ajánlások" jogi természetéről tudnunk kell, hogy nem bírnak kötelező erővel a Tanácsban részes tagállamok számára. "Kötőerejük" az ET.-hez történő csatlakozáskor, a nemzetközi együttműködés fokozására tett általános kötelezettségvállalásból, valamint abból a józan belátásból fakad, hogy az együttműködés eredményességéhez elengedhetetlenül szükséges a közös jogi alap megteremtése.

Közvetetten hat az információs bűnözés elleni küzdelemre az Európa Tanács 1981. évi Adatvédelmi (108. számú) Egyezménye, amely alapul szolgál a hazai 1992. évi LXIII. törvény részletszabályainak kidolgozásához.

A büntetőpolitika felelősségteljes mérlegelés során meghatározza azon védendő érdekeket, amelyeket a büntető törvényhozásnak jogszabályi formába kell önteni.

A szakirodalomban **Irk Ferenc** a büntetőjog által védett érdekeket az értékelés szintje alapján az alábbiakban rendszerezi: "első generációs érdekek, ilyen

az élet, testi épség megóvása, a mozgásszabadság, a nemiség, a tulajdon, az államélet biztonsága, a becsület tiszteletben tartása, második generációs érdekek, ilyen a gazdasági élet, a természet, a közlekedés biztonsága, harmadik generációs érdekek, ilyenek az önrendelkezési jog, az adatvédelem .[44]"

Magam úgy fogalmaznék, hogy a társadalmi együttélés rendjét, a társadalom reprodukcióját, harmonikus fejlődését biztosító büntetendővé nyilvánított magatartások között szükségszerűen fellelhetők azok, amelyek relatív állandósággal jelen vannak a büntető törvényekben. Ezek a társadalmi együttélés alapvető normáit, érdekeit, értékeit (pl. az élet-, testi épség, egészség, a becsület, a tulajdon, a nemi szabadság, a politikai hatalom) védelmezik. Ugyanakkor a társadalmi - gazdasági - politikai változás, és/vagy a műszaki - technikai fejlődés újabb magatartások kriminalizálásának, illetve a szabályozott bűncselekmények enyhébb értékelésének vagy eltörlésének szükségességét veti fel.

A műszaki – technikai fejlődés teremti meg számítógépes környezetben elkövethető visszaélések lehetőségét. E jogsértések sajátosságuk folytán *kihívást jelentenek* a büntető-jogtudomány számára.

A számítógép ugyanis elektronikus adatokkal végzi a programok által irányított műveleteket, ezeket tárolja, továbbítja. Ezen adatok szemmel nem látható, testetlen elektronikus impulzusok. Tartalmuk szerint rendkívül sokrétűek lehetnek, funkciójuk szerteágazó. Jelölhetnek vagyoni értéket, személyhez kötött adatokat, jogi értékelés alapjául szolgáló szöveget, ábrát, táblázatokat stb. Ezen adatokat lehet jogtalanul kifürkészni, módosítani: részlegesen vagy egészében törölni, felülírni, kiegészíteni stb. A beavatkozások az adatállomány megjeleníteni kívánt tartalmát megváltoztatják, amely pénzben kifejezhető vagyoni kárt okozhat vagy más jellegű hátrányt idézhet elő az adatokkal összefüggésbe hozható személy számára. Egy - egy adatállomány jogtalan törlése vagy az elektronikus adatfeldolgozás más módon megvalósuló akadályozása megbéníthat távközlési kommunikációt, gyártási

---

[44] Magyar kriminálpolitikai és rendvédelmi koncepció. Készítői között és szerkesztője: Dr. Irk Ferenc.
Kriminológiai Közlemények 57. Budapest, 1999. 22.l.

tevékenységet, pénzügyi folyamatokat stb. Az adatokat jogtalan gyűjtésével, felhasználásával, továbbításával az adattal érintett személy érdeke sérül stb.

A programok algoritmusok logikus sorozata, amely az adatokkal műveleteket képes végrehajtani. E programok kimunkálása, megalkotása szellemi tevékenység. Ez olyan érték, amely jogosulatlan használattal, másolással, kereskedésével sérthető.

A büntetőjognak tehát az elektronikus adatok, mint sokrétű információk hordozói és az adatok, mint rendszer, azaz a számítógépes szoftver védelmének feltételeit kell kialakítania.

Ezzel összefüggésben a német **Ulrich Sieber**[45] és az amerikai **Cole Durham**[46] a paradigmaváltás szükségességét vetik fel a *büntető-jogtudományban.* Ennek körvonalai az alábbiakban ragadható meg:

- a technika gyors fejlődése a társadalom életét gyorsabb ütemben alakítja át,
- az információ szabad áramlásának biztosítása, amely egy demokratikus berendezkedésű állam létalapja, összhangba kell, hogy kerüljön az információval érintett személy érdekével,
- korábban a büntető-jogtudomány általában a birtokbavehető, testi dolgokra koncentrált, most meg kell teremteni az elektronikus impulzusok, az adatok testetlen és egyben láthatatlan anyagi javak büntetőjogi védelmét,
- ezzel összefüggésben a testetlen, láthatatlan anyagi javak exkluzivítása (személyhez való kötődése) gyengébb, mint a testi javaké, mivel az elektronikus adatfeldolgozás során kezelt adatok a "köz" - szolgálatában is állnak,
- a kriminalizált emberi magatartások fókuszában eddig személy - személy elleni, illetve személy - dolog elleni támadás állott, az elektronikus adatfeldolgozás megjelenésével a személy és a technika vívja küzdelmét.

---

[45] Dr. Ulrich Sieber: The International Emergence of Criminal Information Law id. mű p. 16-17.

[46] Dr. Cole Durham: The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm. International Review of Penal Law. 1993. 1-2. 64. évf. p. 86-93.

Magam úgy vélem, hogy az (elektronikus) adatok védelme a büntetőjog-tudomány egyik területe. Nem kétséges, hogy egyre fontosabb része lesz. Ennek dogmatikai megalapozása, tényállások kialakítása mellett a tulajdon-, és birtokjog körültekintő védelme, illetőleg ennek fejlesztése sem elhanyagolandó.

E külvilágban megjelenő dolgok jelenítik meg, közvetítik a külvilág számára a büntetőjog által védett vagyoni viszonyokat. A tulajdon- vagy jogszerű birtoklás jogi védelme a régmúltból ered. Ez a büntetőjogban relatív állandósággal fellelhető, mivel ez a társadalmi együttélés egyik alapvető normája. A jogfejlődés során általánosan szankcionálást nyernek szerte a világon, megközelítőleg azonos tartalommal az alábbi vagyon elleni magatartások:

a. más vagyonának jogtalan elvételét: lopás, rablás, zsarolás,

b. a jogszerűen átvett idegen vagyonával való jogtalan rendelkezés: sikkasztás,

c. saját vagyon megtévesztés folytán történ átadását: csalás,

d. más vagyonának megrongálását, megsemmisítését: rongálás, és folytathatnánk a sort.

E körben súlyosabb jogi értékelést von maga után, ha ezen vagyontárgyak bizonyos egyedi (pl. muzeális tárgy, régészeti lelőhely, kulturális javak körébe tartozó) jelleggel bírnak.

A büntetőjognak a hatókörét tehát a külvilágba objektivizálódott testi dolgok védelme *mellett*, az emberi szemmel nem látható, fizikai léttel nem rendelkező, csupán adott környezetben tartalommal bíró elektronikus impulzusokra is ki kell terjesztenie.

A paradigmaváltásnak nevezett tényszerű megállapítás *alapja* az, hogy a fizikai léttel bíró, szemmel érzékelhető tárgyak büntetőjogi védelmének hagyományos elve és ennek intézményei nem adaptálhatók teljes egészében az elektronikus adatok védelmében.

Véleményem szerint ennek okai a következők:

1. A fizikai léttel bíró *vagyontárgy* egy - egy tulajdonoshoz vagy jogszerű birtokoshoz kötődik, amelynek valamennyi részjogosultsága (pl. birtoklás, használát)

egyidejűleg csorbát szenved vagy kerül veszélybe egy hagyományos bűncselekmény elkövetésével.

Az immateriális *adatok* esetében a tulajdon, mint jogösszesség többfelé oszlik és e jogösszesség egyes elemei nem ritkán szembeállnak, sőt versenyeznek egymással:

a. az információt létrehozója, összeállítója,

b. az információ jogszerű birtokosa, valamint

c. az adatalany között,

d. az információ szabad áramlásában érdekelt társadalmi érdekek.

Figyelembe kell venni, hogy az a. – b. – c. pontokban felsoroltak között azonosságok is adódhatnak, ami versengésüket kizárhatja.

2. Az elektronikus adathoz, az *információhoz való jogok* sem formájukban, sem tartalmukban nem azonosak a vagyontárgyak tulajdonosának vagy jogszerű birtokosának mindenki mást kizáró jogosultságaival.

Ha így lenne az információ szabad áramlásának elve csorbulna. Ezen elvnek az érvényesülése a társadalom technológiai, tudományos fejlődésének, az anyagi jólét jobbításának elengedhetetlen feltétele.

A számítógépes adatok jogi védelme során, meg kell teremteni azt a rendkívül kényes egyensúlyt az adatalany, és -birtokos vagy -gyűjtő között, valamint az információ szabad áramlásának társadalmi érdeke között. Ezen célhoz kell a büntetőjog eszközrendszerét is alárendelni.

3. Az elektronikus adatok - ahogy erre már fentebb utaltam - *csak meghatározott közegben, meghatározott időben* bír jelentéssel, ezáltal értékkel az adatalany, az adat gyűjtője, más információ birtokos számára. Az információkat e közegből csak társadalmi érdekből lehet kiemelni vagy azokat felhasználni, továbbítani. Ugyanakkor ezen információk jogosulatlan kifürkészése, műveletek végzése, továbbítása, felhasználása elsősorban az adattal érintett személyek, végső soron az egész társadalom érdekét sérti.

Mindezekből látható az, hogy a fizikai léttel bíró, testi dolgok védelmére hivatott büntetőjogi eszköz- és intézményrendszer nem alkalmazható. Eltérő szabályokat kell kialakítani a fenti szempontok figyelembe vételével.

Ennek előrebocsátásával kísérletet teszek az informatikai bűncselekmények közös jogi tárgyának meghatározására.

4. 1. Az informatikai bűncselekmények jogi tárgyáról

Egy adott bűncselekmény sohasem önmagában, hanem valamely *jogi tárgy* sértésében vagy veszélyeztetésében jelent veszélyt a társadalomra.

A büntető-jogtudományban klasszikusaiként tisztelt jogtudósok jogvédte érdekben (Rechtsgut) vagy jogi normában jelölték meg a bűncselekmény jogi tárgyát. Az előbbiek közé tartozott a német **Franz von Liszt**, aki plasztikusan úgy fogalmaz hogy a jogvédte érdek az "bárkinek (Hinz oder Kunz) az érdeke".[47] A svájci **Thormann** és **Overbeck** is ezt határozza meg közös tankönyvében.[48]

A német **Edmund Mezger** különbséget tesz a személy egyéni és társadalmi érdeke között és további tipizálásként idézi **Manigk**-ot, aki viszont materiális (vagyon, tulajdon stb.) és eszmei (mint pl. a szabadság) érdekek közt differenciál.[49]

Ezzel szemben az olasz **Francesco Carrera**[50] és a német **Karl Binding**[51] a jogi normát tekinti a bűncselekmény tárgyának.

A magyar büntető-jogtudományban **Angyal Pál**[52] és **Finkey Ferenc**[53] is a jogvédte érdekben véli megtalálni a jogi tárgy fogalmát. **Hacker Ervin** ehhez hozzáteszi, hogy "csak a materiális jogtárgyaknak van tevékenységi tárgya."[54]

---

[47] Dr. Franz von Liszt: Lehrbuch des Deutschen Strafrechts. Berlin, 1894. s. 49.
[48] Dr. Thormann - Dr. Overbeck: Das Schweizerische Strafgesetzbuch I. Zürich, 1940. 140.l.
[49] Dr. Edmund Mezger: Strafrecht (Zweite Auflage). München und Leipzig, 1933. 198.l.
[50] Dr. Francesco Carrera: A büntetőjogtudomány programja. Budapest, 1878. 51.l.
[51] Dr. Karl Binding: Normen und Ihre Übertretung. I. Leipzig, 1922. s. 353-364.
[52] Dr. Angyal Pál: A magyar büntetőjog tankönyve. I. kötet. Budapest, 1920. 90.l
[53] Dr. Finkey Ferenc: A magyar büntetőjog tankönyve. Budapest, 1902. 183.l.
[54] Dr. Hacker Ervin: A magyar büntetőjog tankönyve. Általános rész. Miskolc, 1936. 115.l.

A mai magyar büntető-jogtudomány közel azonos álláspontot képvisel a jogi tárgy meghatározásában. A bűncselekmény jogi tárgyának azon társadalmi viszonyokat, illetőleg ennek valamely elemét vagy funkcionálási feltételeit tekinti, amelyeket a törvényhozó büntetőjogi védelemre érdemesnek tart. **Földvári József** úgy véli, hogy "a társadalmi viszony mindig emberek közötti viszony, akik társadalmi létük folyamatában vagy mint egyes személyiségek vagy a társadalmi intézmények keretében lépnek fel."[55] E tartalmi meghatározás mellé **Tokaji Géza** kiemeli azt, hogy "formai értelemben jogi tárgy az, amit a büntetőjogi véd, illetőleg a bűncselekmény támad."[56]

A büntetőjog nem egyes személy individualizált érdekeit érdemesíti jogi védelemben, hanem ezen érdekeket azon társadalmi viszonyokba helyezi, amelyekben ezen érdekek, értékek realizálódnak. Nem minden társadalmi viszony élvez büntetőjogi védelmet, hanem csak azok, amelyeket a törvényhozó a társadalmi együttélés megvalósulásához elengedhetetlennek tart.

A jogi tárgy meghatározása, értelmezése kiemelkedő fontossággal bír a büntető-jogtudományban, a törvényhozásban és a jogalkalmazás során egyaránt. **Földvári József** elméleti jelentőségét abban látja, hogy "tárgy nélkül nincs társadalomra veszélyesség, társadalomra veszélyesség nélkül nincs a bűncselekmény".[57]

A hatályos magyar Btk. 10. § (2) bekezdése szerint: " Társadalomra veszélyes az a tevékenység vagy mulasztás, amely a Magyar Köztársaság állami, társadalmi vagy gazdasági rendjét, az állampolgárok személyét vagy jogait sérti vagy veszélyezteti." Törvényi definíció közvetíti felénk azon absztrahált jogi tárgyakat, amelyeket a törvényhozó büntetőjogi védelemre érdemesnek tart.

---

[55] Dr. Földvári József: A magyar büntetőjog. Általános rész. Budapest, 1997. 93.l.

[56] Dr. Tokaji Géza: A bűncselekménytan alapjai a magyar büntetőjogban. Budapest, 1984. 106.l.

[57] Dr. Földvári József: A magyar büntetőjog. Általános rész .... id.mű 54.l., és Dr. Békés Imre - Dr. Földvári József - Dr. Gáspár Gyula - Dr. Tokaji Géza: Magyar büntetőjog ..... id. mű 89.l.

A társadalomra veszélyesség objektív kategória. A törvényhozó egyes cselekmények e tulajdonságát felismeri, értékeli, azaz léte megelőzi a jogi szabályozást és a törvényhozó döntését követő jogi szabályozással sem veszti el e tulajdonságát.[58]

Korábbi felfogások szerint a társadalomra veszélyesség normatív kategória. E koncepcióból következően a jogi szabályozással a tényleges társadalomra veszélyesség és a jogi értelemben vett társadalomra veszélyesség már elkülönül egymástól. A tényleges társadalomra veszélyesség a jogi szabályozás hiányában a büntetőjog számára irrelevánssá válik, ezzel szemben a jogban értékelt társadalomra veszélyesség a bűncselekmény fogalom középpontjába kerül.[59] Ezen elméleti problémán polemizálva **Tokaji Géza** nem választja szét a társadalomra veszélyesség ontológiai és normatív jellegét, hanem ennek egységét hangsúlyozva kijelenti, bár az ontológiai veszélyesség normatív mutatkozik meg számunkra, színeződik is, de megjelenésében az ontológiai és a normatív társadalomra veszélyesség, mint egység jelenik meg.[60] Véleményem ez utóbbi megállapításhoz áll közelebb. Elismerve azt, hogy a törvényi tényállás egy valóságos társadalomra veszélyes cselekménytípust fogalmaz meg, amely létezése miatt lett büntetendővé nyilvánítva. Másfelől a cselekmény tényleges társadalomra veszélyesség csupán a büntetőjog számára releváns. E relevancia azonban időleges, hiszen a cselekmény megítélése koronként változhat, súlytalanná is válhat. Esetleg más jogág (pl. a szabálysértési jog) számára értékelésre érdemessé válhat.

Összefoglalásként elvi éllel rögzíthető, hogy ha van olyan társadalmi viszony, amelynek létezéséhez társadalmi érdek fűződik és ez a társadalmi viszony valamely cselekmény által sérül vagy ennek veszélye áll fenn, akkor a jogalkotó törvényi tényállás alkotásával adja tudtára a társadalom számára.

---

[58] Dr. Földvári József: A magyar büntetőjog. Általános rész ..... id. mű 79.l.
[59] Dr. Békés Imre: A gondatlanság a büntetőjogban. Budapest, 1974. 207-210.l.
[60] Dr. Tokaji Géza: A bűncselekménytan alapjai a magyar büntetőjogban ..... id. mű 119-120.l.

Nem csekély felelősség abban dönteni, hogy a társadalom számára hátrányos magatartás eléri-e a jogi, ezen belül a büntetőjogi reakció szintjét.

Györgyi Kálmán - bár más témában, ám elvi éllel - az alábbiakban összegzi a büntetést érdemlőség feltételeit:

a. a fenyegetett érdek védelmet érdemlősége,

b. A büntetés szükségessége, ami annyit tesz, hogy a büntetőjogi eszközök alkalmazásának nélkülözhetetlennek kell bizonyulnia,

c. A büntetés alkalmassága, ami annyit jelent, hogy a büntetőjog eszközeinek alkalmasnak kell mutatkoznia. [61]

Az *informatikai környezet* egyfelől hagyományos értékek viszonyok színtere, pl. anyagi viszonyok, személyiségi jogok. Másfelől maga is új értékéket hoz létre pl. elektronikus kereskedelem vagy az elektronikus posta titkossága, biztonsága.

Az előbbi körben arra a kérdésre kell megfelelő választ adni, hogy van-e a hagyományos értékeket sértő elkövetési magatartások mellett olyan újfajta a társadalomra veszélyes tevékenység, amelyet szankcionálnia kell a törvényhozónak. Már itt felhívjuk a figyelmet a tényállások megkettőzésének veszélyére.

A számítástechnika által teremtett új értékek, érdekek közül pedig a törvényhozónak a büntetőjogi védelemre érdemes értékeket kell kiválasztania.

Ez utóbbi kapcsán megállapíthatjuk, hogy különböző országok többféle informatikai jogsértést kriminalizálnak.

Politikai érdekek, kulturális és jogi tradíciók, a jogi, ezen belül a büntetőjogi felelősségrendszer összhangjának követelményei, esetleg más szempontok figyelembe vételével kell kialakítania a jogalkotónak az álláspontját.

A büntető-jogtudományban a vizsgálódás első lépése a bűncselekmény tárgyának meghatározása.

A tárgy definiálása során az absztrakció fokától függően megkülönböztethetünk:

---

[61] Dr. Györgyi Kálmán: A büntetőjog és a modern orvosbiológia. JK. XXXIX. 1989.203-209.l.

- általános jogi tárgyat. Ezt **Finkey Ferenc** "közvetett" jogi tárgyként határozza meg. Ez azt fejezi ki, hogy minden bűncselekmény közvetett támadás a jogrend ellen.[62] A jogrend konkrét társadalmi viszonyt érő támadással sérthető vagy veszélyeztethető.
- A különös tárgy, másképpen csoporttárgy az életviszonyok az előbbinél egy szűkebb köre, amelyet a Btk. már fentebb idézett rendelkezése határoz meg.
- Egyedi tárgyként az adott bűncselekmény által konkrétan támadott társadalmi viszony definiálható.

Az informatikai visszaélések jogi tárgyának tisztázásához az elektronikus adatfeldolgozás által közvetített társadalmi viszonyt kell meghatározni. Ehhez pedig e hasznos tevékenység funkciójából kell kiindulnom.

A számítástechnikai rendszerek információ rögzítésére, feldolgozására, tárolására, továbbítására szolgálnak. Az elektronikus adatfeldolgozás- és adatátvitel egymásra épülő műveletek, feladatok sorozatát jelentik. E szigorúan racionálisan létrehozott rendszernek, illetve működésének magas színvonalú technikai feltételei vannak. Ugyanakkor mind az elektronikus adatfeldolgozás résztevékenységeit, mind annak egészét jogszabályok övezik, biztosítják. Ilyen jogszabályok hazánkban:
- az 1/1981. (I. 27.) BM. rendelet a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről;
- az 1/1983. (X. 13.) KSH. rendelkezés a statisztikai adatok számítástechnikai eszközök útján végzett rögzítéséről, feldolgozásáról, tárolásáról, továbbításáról;
- a 3/1983. Legfőbb Ügyészi utasítás a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről;
- az 1/1986. (II. 1.) Ipari miniszteri rendelet a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről;

---

[62] Dr. Finkey Ferenc: A magyar büntetőjog tankönyve. Budapest, 1914. 236.l.

- továbbá számítástechnikai rendszert működtetők, adatokat felhasználók által kibocsátott belső szabályzatok, utasítások és más jogi normák. Emellett közvetetten az adat- és titokvédelmi törvények, és egyéb jogi normák.

A jogszabályok összevetéséből általános megállapítások tehetők:
ezek meghatározzák az elektronikus adatfeldolgozás módját, terjedelmét, időbeli határait, a feldolgozást végzők jogait, kötelességeit, az adattovábbítás irányát, az adathordozók védelmét stb. Ebből következik, hogy az elektronikus adatfeldolgozás rendjének kialakulnak konstans elemei, amelyek beépülnek az e körben születő jogi szabályokba, és amelyek e tevékenység technikai feltételeinek megteremtésére ösztönöznek. Kiemelkedően fontos társadalmi - gazdasági érdek az egyre bővülő és jelentősebbé váló elektronikus adatfeldolgozás- és adatátvitel folyamatának, technikai feltételeinek, az ott kezelt információknak biztonsága, védelme, zavartalansága, azaz az elektronikus adatfeldolgozó rendszer integritásának biztosítása.

Ez képezi - véleményem szerint - a számítógépes környezetben elkövetett bűncselekmények *jogi tárgyát.*

Az elektronikus adatfeldolgozó rendszer sokrétű funkciójából következően, az e rendszerek elleni támadás általában más társadalmi viszonyt is sért, ezáltal az informatikai bűncselekmények általában *kettős jogtárggyal* jellemezhetők; pl. számítógépes csalás esetén az elektronikus adatfeldolgozás integritása, biztonsága mellett a vagyoni viszonyok is sérelmet szenvednek, vagy személyes adatok sérelmére végrehajtott magatartás esetén a személyes adatok titkosságához fűződő érdek is.

A jogi tárgy tisztázását követő kérdés, hogy vajon e bűncselekmények alkothatnak-e egy *önálló fejezetet* vagy sem.

A nemzetközi jogalkotás vázlatos áttekintése során találunk példát a bűncselekmények egy különálló kódexbe, továbbá a büntető törvénykönyv egy önálló fejezetébe gyűjtött vagy a Különös részben szétszórtan beemelt tényállásokra.

Az *Egyesült Királyságban* 1990-ben lép hatályba az ún. Computer Misuse Act, amely több a számítógépes visszaélés körébe sorolt magtartást kriminalizál. *Franciaországban* a Code Penal egy egész fejezetet szentel ezen bűncselekményeknek, ez a III. fejezet, és az itt található 462.2. - 462.9. §-ok. *Ausztriában, Dániában, Finnországban, Magyarországon, Németországban, Spanyolországban, Svájcban és Svédországban* a hagyományos jogi tárgyat védő tényállások mellett szerepelnek az új típusú tényállások.

A számítógépes környezetben megvalósuló bűncselekmények büntető törvénykönyvben történő szabályozása évek, netán évtizedek során fog realizálódni. A technikai fejlődés előrehaladtával újabb, és újabb jogsértések tűnnek fel. Gondoljunk arra, hogy az 1989-ben közkinccsé váló Európai Tanács Ajánlásban még nem szerepel nevesítve a bankkártyával visszaélés, vagy arra, hogy az e-mail (elektronikus posta), mint új közlésforma, az Interneten folytatott elektronikus kereskedelem, a készpénzforgalom fokozatos háttérbe szorulása további jogi, így büntetőjogi problémákat vetnek majd fel.

Mindezek előrebocsátásával úgy gondolom, hogy rövid távon az informatikai deliktumok hagyományos Különös részi struktúrába kerülnek. Hosszabb távon a bűncselekmény tárgyi oldalán mutatkozó hasonlóságok, szoros összefüggések miatt e bűncselekmények a büntető törvénykönyvek *önálló fejezetét* önálló fejezetét fogják alkotni.

Ennek elméleti indoka a bűncselekmény tárgyi oldalán keresendő. Ahogy a közlekedési büntetőjog tényállásainak legfőbb közös sajátja az, hogy "alkalmazásának alapját a közlekedési szabályok megszegése képezi" és ez "érdemben fontosabb összetartó tényező, mint amennyire más faktor az egyes cselekmények egymástól való megkülönböztetésére indokot nyújthat"[63], úgy az elektronikus adatfeldolgozás integritásának, biztonságának megsértése, mint büntetőjogi védelemre érdemes társadalmi érdek az egyik közös jellemző. A másik közös vonásuk az informatikai bűncselekmények azonos elkövetési vagy tevékenységi tárgya, azaz az elektronikus impulzus, mint számítógépes adat. A

tárgyi oldalon mutatkozó harmadik közös sajátosságuk az elkövetési magatartások hasonlósága (szinte valamennyi jogsértés adat-, és/vagy programmanipuláció révén valósul meg stb.).

Mindezek megalapozzák az informatikai bűncselekmények önálló fejezetbe foglalását.

4. 2. Az informatikai bűncselekmények tevékenységi tárgyáról

A jogi tárgyak általában közvetett jellegűek, mivel zömében csak valamely, a jogi tárgyat megtestesítő tevékenységi tárgyon keresztül sérthetők vagy veszélyeztethetők.

Ha jogi tárgy a külvilágban érzékelhető dolgon vagy személyen szimbolizálódik úgy a bűncselekménynek *tevékenységi tárgya* van. Ellenben immateriális bűncselekmények esetében tevékenységi tárgyról nem beszélhetünk.

A tevékenységi tárgy, egyfelől a jogi tárgyat képező társadalmi viszony előfeltétele pl. egy vagyontárgy a tulajdon- vagy a birtokviszonyt testesíti meg, Másfelől a védeni kívánt társadalmi viszony fizikai kifejeződése pl. az okirat.

Földvári József azt az álláspontot képviseli, hogy ez a szembeállítás mesterkélt, mivel a társadalmi viszonyok létezése elképzelhetetlen alanyok vagy más hordozók nélkül.[64]

Békés Imre és **Tokaji Géza** szerint e szétválasztásnak van értelme. Tokaji Géza egy példával illusztrálja véleményét. Szerinte a lopás bűncselekménye a tulajdonviszonyokat sért, ám a jogtárgysértést a dologelvétel, mint elkövetési magatartás teremti meg.[65] Békés Imre a tevékenységi tárgyat a bűncselekmény tárgyi elemei közé viszi. A jogi tárgy a "bűncselekmény tárgya" körében marad.[66]

---

[63] Dr. Viski László: Közlekedési büntetőjog. Budapest, 1974. 268.l.
[64] Dr. Földvári József: A magyar büntetőjog. Általános rész ..... id. mű 96-97.l.
[65] Dr. Tokaji Géza: A bűncselekménytan alapjai ..... id. mű 104.l.
[66] Dr. Békés Imre - Dr. Györgyi Kálmán - Dr. Papp György: Büntetőjog (Államigazgatási főiskolai jegyzet).
Budapest, 1980. 32.l.

Ez a büntetőeljárásban, a bizonyítás során nyer értelmet. A tényállás - akár tárgyi, akár alanyi - elemeit kell hatóságnak bizonyítani.[67]

E kérdés kapcsán úgy vélem, hogy a bűncselekmény tárgyának felosztása jogi és tevékenységi tárgyra akkor tartható, ha ez a bekövetkezett cselekmény *minősítéséhez*, mint büntetőjogban elsősorban releváns kérdés megválaszolásához hozzájárul.

Az elhatárolási probléma feloldásához, bűncselekmény - egység vagy halmazat megítéléséhez stb., majd az ebből eredő jogkövetkezmények (pl. büntetés-végrehajtási fokozat, visszaesés megállapíthatósága) érvényesítéséhez a bűncselekmény által támadott jogi tárgy tisztánlátása nélkülözhetetlen. Ekkor a tevékenységi tárgy leválasztása a jogi tárgyról nem feltétel. Elvitathatatlan ugyanakkor, hogy a büntetőjogban értékelt támadás az elkövetési tárgyon keresztül sérti vagy veszélyezteti a jogi tárgyat, illetőleg a támadás a jogi tárgyon realizálódik.

A büntető-jogtudomány tevékenységi tárgyként napjainkig általában *testi tárgyakat* illetve *személyeket* definiált. **Angyal Pál** idézi a dolog *liszti-schmidti* meghatározását, e szerint a testi dolog a „természetnek emberi uralom alá vethető testi darabja."[68]

A *fizikai léttel bíró dolog* sajátosságai az alábbiak:

a. a dolog a külvilágban testet öltött és látható objektum.

b. Általában meghatározható vagyoni értékkel bír.

c. A jogi védelem egyediségüket fogja át.

d. Az ellene irányuló támadás a külvilágban változást idéz elő.

Pl. az ingó dolog eltulajdonítását megelőzi a dolog elmozdítása, majd elvitele a bűncselekmény helyszínéről. A dolog megrongálása (akár rongálással, akár a dolog szétszerelésével), általában állagkárosodással jár együtt.

E jellemzőkkel összevetem *az adat, mint elektronikus impulzus* sajátosságait:

---

[67] Dr. Tokaji Géza: A bűncselekménytan alapjai ..... id. mű 105 - 106.l.

[68] Dr. Angyal Pál: A lopás. (A Magyar Büntetőjog Kézikönyve 10. kötet.) Budapest, 1932. 22.l.

Ad a. az elektronikus adat immateriális és láthatatlan. Külvilágban történő megjelenítéséhez technikai eszközök és számítógépes szoftverek szükségesek.

Ad b. Az adat vagyoni értéke általában nem ragadható meg. Egy-egy adat saját környezetében, közegében meghatározott helyen és időben rendelkeznek értékkel. Míg a számítógép vagyoni értéke számottevő, amely befolyásolja az elkövető cselekményének a jogi minősítését, addig az adathordozók értéke nem jelentős.

Ad c. Jogi védelme is akkor merül fel, ha e közegből jogosulatlanul "kiemelni", kifürkészni, törölni, továbbítani kívánják.

Egyediségük irreleváns, korlátlanul másolhatók.

Ad d. Az elektronikus adat, mivel immateriális és láthatatlan, az ellene irányuló támadás sem idéz elő külvilágban érzékelhető változásokat.

A számítógépben vagy az adathordozón tárolt adatok "ellopása" nem jelenti az adat "elvitelét".

Általában az adatok megrongálása sem eredményez külvilági változást. Kivéve, ha a számítógépet vagy az adathordozót erőszakos fizikai hatás éri.

Viszont az adatok megrongálásáról beszélünk akkor, ha azokat megváltoztatják, vagyis felülírják, kiegészítik, továbbá részben vagy egészben törlik.

A számítógépes környezetben elkövetett visszaélések kriminalizálása körében a büntető-jogtudomány néhány sajátos problémával kerül szembe:

1. a számítógépes környezeten elkövethető visszaélések jogi minősítéséhez *meg kell ismerkednünk* az egyes magatartások speciális vonásaival, technikai alapjaival.

Majd ez alapján eldönthető, hogy az adott konkrét cselekmény beilleszthető-e egy absztrakt tényállás keretei közé vagy sem.

Sajnos, meglehetősen szerény az a hazai szakirodalom, amely támaszt nyújthatna a jogalkalmazás során felvetődő kérdések megnyugtató tisztázásához.

2. E vizsgálódás nélkülözhetetlen, hiszen minden egyes új vonásokkal bíró jogsértések értékelésékor fennáll - a fentebb már említett - *tényállások megkettőzésének a veszélye.* Erre már találunk negatív példát a magyar Btk.-ban, amely

számtalan csalás jellegű magatartás önálló bűncselekményként való értékel (pl. hitelezési csalás Btk. 297/A. §, alaptőke vagy törzstőke csorbítása Btk. 298/B. §, tőkebefektetési csalás Btk. 299/B. §, piramisjáték szervezése Btk. 299/C. § stb.)

3. Ha a jogértelmezés ismert módszereivel arra a következtetésre jutunk, hogy az adott konkrét tevékenység nem minősíthető a hatályos tényállások szerint, akkor - a nullum crimen sine lege garanciális elve miatt - új tényállások meghatározására van szükség.

4. A jogalkotás során fokozottan figyelnünk kell a nyugat - európai megoldásokra, egyrészt ezen országok az információs technológia területén még előttünk járnak, így a visszaélések is - elvileg - korábban észlelhetők, így az ezekre adott büntetőjogi válasz is például szolgálhat. Ez szakmai szempont.

Másrészt az Európai Unióhoz való csatlakozás politikai pozícióit erősíti az OECD- vagy Európa Tanács jogi normáinak átvétele. Ez utóbbi hazánk integrációs politikájának szándékát erősíti.

5. TIPIZÁLÁSI TÖREKVÉSEK A NEMZETKÖZI SZAKIRODALOMBAN

A számítógépes környezetben elkövetett bűncselekmények fogalmát illetően többféle elnevezés ismert a szakirodalomban.

Korábban általánosan használatos volt a számítógépes bűnözés terminológia. A német és az angol nyelvterületen ennek megfelelően "der Computerkriminalitat" illetve a "Computer Crime" volt ez a fogalom, míg a francia nyelvű országokban informatikai bűnözés (la delinquance informatique) meghatározás válik elfogadottá. A kilencvenes években az angolszász szakirodalomban a számítógépes környezetben elkövetett bűnözés (computer-related crime) elnevezés olvasható, amely tartalmi különbözőséget is jelöl. Utal arra, hogy léteznek olyan bűncselekmények, amelyeknek nem a számítógép a közvetlen tárgya vagy a célja. Ezek közé sorolható a szoftver elleni szerzői jogot sértő cselekmények vagy az elektronikai félvezetők jogosulatlan megszerzése és kereskedelme.

Balog Zsolt György felhívja a figyelmet arra, hogy a "tapasztalatok szerint nemcsak számítógépek, hanem kommunikációs berendezések, ... egész kommunikációs rendszerek, adatátviteli hálózatok lehetnek érintve"[69] a bűncselekmények elkövetésével.

A számítógépes bűnözés a bűncselekmények konkrét megjelenési formáinak, valamint a veszélyeztetett jogtárgyak sokszínűsége miatt csak gyűjtőfogalommal írható le.

A szakirodalomban (még) nem született olyan fogalom, amely általánosan elfogadottá válna. Ennek magyarázatául az szolgál, hogy egyfelől ez a kriminális jelenség új keletű, másfelől a számítástechnika fejlődésével a veszélyeztetett értékek és érdekek köre is gyarapszik.

---

[69] Dr. Balogh Zsolt György: Jogi informatika ..... id. mű 258.l.

5. 1. A számítógépes bűnözés meghatározására tett kísérletek

A hetvenes évek elején a német **Rainer Mühlen** számítógépes bűncselekménynek tekint minden olyan magatartást, melynek eszköze vagy célja a komputer.[70]

Hazánkban **Polt Péter** hívja fel a figyelmet a tudományos közélet figyelmét erre az új kriminális jelenségre. Hasonlóan vélekedik arról, hogy a számítógép egyszerre lehet a bűncselekmény tárgya és eszköze.[71]

Az osztrák **Walter Jaburek** és **Gabriele Schmölzer** szerzőpáros Mühlen megállapítását finomítja azzal, hogy a számítógépet a cselekmény közbenső vagy végső céljának fogták fel. Ennek megfelelően, ha az elkövető a számítógépre irányuló magatartását pl. az adatlopást az adatok másolásával befejezi, úgy cselekménye végső célként jelenik meg a számítógép vonatkozásában. Ugyanakkor, ha bűncselekményét pl. a manipulált számítógépes adatokkal vagy programokkal hajt(at)ja végre, úgy a komputer csak, mint közbenső célként határozható meg.[72]

A dél - afrikai **Michels** korai meghatározása szerint a számítógépes visszaélés felöleli a gép használatát, mint célt és azt a szituációt, amelyben a jogtalan hozzáférés megvalósul. Később a jogosulatlan információ- és pénzszerzést, a hardver- és szoftverlopást, valamint a szabotázst és a hitelkártyacsalást is idevonja.[73]

Hazánkban kezdetben **Pusztai László**[74], és jómagam[75] is a számítógépes bűncselekmények négy fő alaptípusa között tettünk különbséget: a számítógépes visszaélést, az adatkikémlelést, a szabotázst és a gépidőlopást.

---

[70] Rainer von Mühlen: Computer - Kriminalität, Gefahren und Abwehrmassnahmen, W-Berlin 1973. s.30.
[71] Dr. Polt Péter: A számítógépes bűnözés. BSZ. XXI. 1983. 6. 60-64.l.
[72] W. Jaburek - G. Schmölzer: Computer - Kriminalität, Wien 1985. s. 20. und s(n). 22-23.
[73] Revue ..... p. 553.
[74] Dr. Pusztai László: Számítógép és bűnözés. KKT. XXVI. kötet. Budapest, 1989. 106-107.l.
[75] Dr. Nagy Zoltán: Az informatika és a büntetőjog. MJ. 38. 1991. 1. 21-23.l. és Dr. Nagy Zoltán: A számítógépes bűnözés. CW-Sz. 5. 1990. 41. 16-19.l.

A számítógépes visszaélés jelenti az elektronikus adatfeldolgozási tevékenység minden olyan jogellenes befolyásolását, amelynek célja jogosulatlan vagyoni előny szerzése az elkövető vagy általa más számára. Az adatkikémlelés körébe tartozik részint a számítógép adatainak, részint programjainak jogosulatlan megszerzése. A szabotázs az elektronikus adatfeldolgozási tevékenység jogosulatlan akadályozását foglalja magában. A gépidő - lopás pedig nem jelent más, mint a számítógép jogosulatlan használatát, amely a számítógép üzemeltetőjének kárt okoz. (Magam újabb, a technikai fejlődést követni igyekvő felfogása a következő fejezet bevezetéseként olvasható.)

A francia **Raymond Gassin** az informatikai bűncselekmények tárgyaként megkülönböztet informatikai szabotázs, és informatikai kalózkodás között. Az előbbi csoportba a technikai merénylet, illetve az erőszakkal nem járó kárt okozó cselekmények tartoznak. Az utóbbi csoportban a gépidő – lopás, valamint a software és az információ csalárd eltulajdonítása szerepel. Felfogásában a számítógép lehet a bűncselekmény aktív eszköze (pl. csalás elkövetéséhez) vagy passzív eszköze (pl. a pénzkivételi automata manipulálásához). Ehhez hozzáteszi, hogy számítógéppel a személyiségi jogot sértő bűncselekmény is megvalósítható.[76]

A svájci **Kurt Bauknecht** a számítógépes manipulációkat, a titkos kémkedést, a gépidő - lopást és a szabotázs cselekményeket sorolja ebbe a kategóriába.[77]

A japán **Atsushi Yamaguchi** majdnem ugyanezeket a típusokat említi. Nála az adatmanipuláció, az adatlopás, a komputer jogosulatlan használata és a szabotázs alkotja a számítógépes bűncselekmények csoportját. Bár megjegyzi azt is, hogy további komputeres jogsértések is ismertek, de azok kívül esnek ezen a körön.[78]

A belga **Jean Spreutels** a számítógépes szabotázson, az adat vagy program kikémlelésén, az adat vagy program manipuláción, a komputer jogosulatlan használatán túlmenően a számítógépes hamisítás és a rendszerbe történő

---

[76] Raymond Gassin: Az informatika büntetőjoga. MJ. 35. 1988.2. 164-172.l.
[77] Revue ..... p. 592.
[78] Revue ..... p(s). 434-435.

jogosulatlan behatolás felvételével bővíti a számítógépes bűncselekmények meghatározását.[79]

A német **Manfred Möhrenschlager**nél az adat vagy program manipuláció, a szabotázs és adatváltoztatás, a gépidő - lopás mellett megjelenik a személyes adatokat veszélyeztető támadás is.[80]

Összefoglalásként megállapítható, hogy a fenti tipizálások megfelelnek a hetvenes évek technikai feltételei által nyújtott jogellenes magatartások bűncselekményként történő értékeléséhez.

A számítógépes csalást, az (adat) kikémlelést, a szabotázst, a gépidő - lopást nevezhetjük az *első generációs informatikai bűncselekményeknek.*

A 80-as évek második felétől a bűncselekmények köre bővül.

Az osztrák **Gabriele Schmölzer** immár **Peter Schick**-kel karöltve rendszerezi az eddigiekben megismert magatartásokat:

a. támadás a hardver ellen: - jogosulatlan belépés,
- gépidő - lopás,
- a mikrochip jogtalan másolása,

b. támadás a szoftver ellen: - szoftverlopás,
- programmanipuláció,

c. támadás az adat ellen: - adatmanipuláció,
- adatlopás,
- visszaélés az adatfeldolgozási tevékenységgel. [81]

Az egyesült államokbeli **Adler-Mueller-Laufer** szerző triász a számítógépes bűncselekmények alábbi típusait határozzák meg:

a. számítógépes csalás;

b. számítógépes kikémlelés;

c. számítógépes szabotázs;

---

[79] Revue ..... p(s). 164-172.
[80] Revue ..... p. 321.
[81] Revue ..... p. 134.

d. számítógépes hacking;

e. számítógépidő-, szoftver és hardver lopás.[82]

Az angol **Martin Wasik** csoportosításában az alábbi magatartásokat sorolja e körbe:

a. jogosulatlan hozzáférés a számítógépben tárolt adatokhoz vagy programokhoz;

b. számítógépes csalás;

c. adatok vagy programok jogosulatlan elvitele;

d. a számítógépidő- és szolgáltatás jogosulatlan használata;

e. rombolás vagy károkozás.[83]

A **Skót Jogi Bizottság** a számítógépes visszaélések alábbi formáit határozza meg:

a. adatok vagy programok meghamisítása anyagi vagy egyéb előnyszerzés céljából;

b. jogosulatlan hozzáférés lehetővé tétele;

c. a számítógép lehallgatása;

d. információlopás;

e. adattárolók jogosulatlan másolása;

f. a számítógépidő vagy eszközök jogosulatlan igénybevétele;

g. adatok vagy programok szándékos vagy gondatlan törlése;

h. az illetékes vagy törvényes felhasználó számára a hozzáférés megtagadása.[84]

A OECD által kiküldött ad hoc bizottság 1983 - 1985. között elemzi, majd összegzi az európai judikatúra tapasztalatait. Megállapításaikkal iránymutatást kívánnak adni a számítógépes környezetben elkövetett bűncselekmények megismeréséhez és kodifikálásához. A bizottság az alábbiakban rendszerezi a jogsértéseket:

---

[82] Freda Adler - Gerhard O.W. Mueller - Williams S. Laufer: Criminology, McGraw Hill Inc. New York etc. 1991. p. 292.

[83] Dr. Martin Wasik: Crime and the Computer, Oxford 1991. p.(s) 1-2. és p(s). 24-64.

[84] Ian Lloyd: Computer Crime, New Law Journal 08. 08. 1986. p(s). 761-762.

a. számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elrejtése jogtalan vagyoni eszközök vagy más értékek megszerzése céljából;
b. számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elrejtése hamisítás céljából;
c. számítógépes adatok és/vagy programok bevitel, módosítása, törlése vagy elrejtése vagy a számítógépbe történő bármely más beavatkozás abból a célból, hogy a számítógépes vagy telekommunikációs rendszerek funkcióinak megakadályozása céljából;
d. a védett számítógépes programok tulajdonosai exkluzív jogainak megsértése a program jogosulatlan hasznosítása vagy forgalomba hozatala révén;
e. a számítógépes vagy telekommunikációs rendszerbe az arra jogosult engedélye nélkül vagy a biztonsági intézkedések megsértésével vagy más tisztességtelen vagy bűnös szándékkal történő belépés vagy annak lehallgatása.[85]

Az **Európa Tanács** a nyolcvanas évek második felében szakértői bizottságot hoz létre abból a célból, hogy az felmérje a számítógépes bűncselekmények realitását, valós veszélyeit, összegezze az erre vonatkozó ismereteket, és dolgozzon ki egy ajánlást a kriminalizálandó magatartásokról a tagországok számára. Az Ajánlás 1989-ben kerül kibocsátásra. Ebben a szakértői testület kerüli a számítógépes bűncselekmények közös ismérveinek fogalomszintű meghatározását. Helyette egy listát állít össze, amelyben az eddig napvilágot látott számítógépes környezetben megvalósítható deliktumok szerepelnek.

Ezt a listát vitatja meg az 1992-ben Würzburgban tartott konferencia az információ - technológiai bűnözésről, majd az 1994-ben rió de janeiroi AIDP Világkongresszus.

Az **ET. (89) 9. sz. Ajánlásában** szerepel egy minimális lista, azokról a cselekményekről, amelyeket leginkább javasol szankcionálni, továbbá a minimum

---

[85] OECD Computer - Related Criminality: Analysis of Legal Police. Paris, 1986. (továbbiakban: OECD - Analysis) p. 28.

listát kiegészítő fakultatív lajstrom. Jelentősége miatt indokolt a bűncselekmények puszta felsorolása mellett azok rövid meghatározásait is nyújtani.

Valamennyi alább említett bűncselekmény büntetőjogi üldözésének elemi feltétele az, hogy az elkövetés *szándékosan* történjen.

I. Az ET. minimális listája:

a. A számítógépes csalás: adatok, programok bevitele, megváltoztatása, törlése, elrejtése, vagy más az elektronikus adatfeldolgozási folyamat befolyásolását eredményező magatartás, amellyel az elkövető egy harmadik személynek gazdasági vagy vagyoni hátrányt okoz, illetve amelynek célja az, hogy az elkövető önmaga vagy más számára gazdasági, illetőleg vagyoni előnyhöz jusson. Az Ajánlás alternatív javaslata: más személyt vagyonától megfosszon.

b. A számítógépes hamisítás: adatok, programok bevitele, megváltoztatása, törlése, mentése vagy más az elektronikus adatfeldolgozási folyamat befolyásolását eredményező beavatkozás, amelynek révén megvalósul a hazai jogban meghatározott hagyományos hamisítás bűncselekménye.

c. A számítógépes adatokban és programokban történő károkozás: az adatok és/vagy programok jogosulatlan törlése, rongálása, károsítása, mentése.

d. A számítógépes szabotázs: olyan adatok és/vagy programok bevitele, megváltoztatása, törlése vagy más befolyásolása a számítógépes rendszereknek, amelynek célja, hogy annak telekommunikációs funkcióját akadályozza.

e. A jogellenes behatolás: a számítógépes rendszerbe vagy hálózatba történő jogosulatlan bejutás a biztonsági intézkedések megsértése révén.

f. A jogellenes titokszerzés: a számítógépes rendszerből vagy hálózatból jogosulatlan tudomásszerzés technikai eszközökkel.

g. Védett számítógépes programok jogellenes másolása: a jogi oltalommal bíró programok jogosulatlan reprodukálása, és értékesítése.

h. A félvezető topográfiák jogellenes másolása: a jogi oltalommal bíró félvezető topográfiák jogosulatlan reprodukálása, azok gyártása, kereskedelmi értékesítése, és importja, akár e termékek felhasználása céljából.

Az ET. fakultatív listáján szereplő cselekmények úgyszintén akkor kriminalizálandók, ha elkövetésük *szándékos*. Ezek:

a. A számítógépes adatok és/vagy programok megváltoztatása: ha jogosulatlan valósul meg.

b. A számítógépes kémkedés: kereskedelmi vagy üzleti titok jogosulatlan vagy törvényes felhatalmazás nélküli megszerzése, nyilvánosságra hozatala, mással való közlése azzal a céllal, hogy a titok jogosultjának gazdasági hátrányt okozzon, illetve a titok megszerzésével önmaga vagy más számára jogtalan előnyt szerezzen.

c. A számítógép jogellenes használata: a számítógépes rendszerek, és hálózatok jogosulatlan igénybevétele során az elkövető:

c1. jelentős kár okozását kockáztatja a jogosult sérelmére, vagy magát a rendszert, illetve funkciójának ellátását kockáztatja, vagy

c2. azzal a szándékkal cselekszik, hogy a jogosultnak, a rendszerben, illetve annak funkciójában kárt okozzon vagy

c3. ténylegesen kárt okoz a jogosultnak, a rendszerben annak funkciójában.

d. Védett programok jogellenes használata: a program olyan jogosulatlan használata, amely felöleli annak jogosulatlan megszerzését önmaga vagy más számára, továbbá minden olyan használat, amely a tulajdonos jogait sérti.[86]

A rendőrségi statisztikák végigtekintése igen tanulságos. Nemcsak a kriminálmorfológiai elemzések miatt, hanem azért is, mivel a büntetőjogi gyakorlat tapasztalatait jelzi. A **holland bűnügyi rendőrség** 1981. óta regisztrálja a számító-

---

[86] Council of Europe Legal Affairs: Computer - Related Crime. Recommendation No.R. (89) 9. Strasbourg, 1990. ISBN 92-871-1792-6 (továbbiakban: CE Recommendation (89) 9. p(s). 36-69..Revue ..... p(s). 673-680. (francia nyelven) és p(s). 681-690. (angol nyelven),
Dr. Nagy Zoltán: Konferencia az információtechnikai bűnözésről. MJ. 40. 1993. 2. 102-104.l.
Dr. Kertész Imre - Dr. Pusztai László: A komputerbűnözés és az információs technológiával kapcsolatos egyéb bűnözési fajták. ÜÉ. 29. 1993.4. 17-18.l., vagy
Dr. Csonka Péter: Council of Europe Activities Related to Information Technology ..... Information & Communications Technology Law, Vol.5. No.3, 1996. p(s).180-186.82.

gépes bűncselekményeket. Első ízben az elkövetés eszközének, és céljának megkülönböztetésével. 1987-től kezdve már új csoportosítást alkalmaznak:

1. számítógépes környezetben elkövetett hagyományos és új típusú bűncselekmények, amelyek eszköze komputer;

2. számítógépes csalás;

3. számítógépes terrorcselekmények:

- jogosulatlan behatolás,
- vírusok és ehhez hasonlatos programok használata,
- egyéb tevékenységek, pl. fizikai támadás;

4. számítógépes kalózkodás;

5. egyéb számítógépes bűncselekmények, amelyek az 1. ponthoz nem sorolhatók. [87]

A **német bűnügyi rendőrség** 1987-ben átdolgozott statisztikájában "a számítógépes bűnözés" elnevezés alatt az alábbi számokon a következő bűncselekmények szerepelnek:

- 5163. pénzkiadó illetve pénztár-automatákkal kapcsolatos csalás,
- 5175. számítógépes csalás;
- 5430. bizonyíték jellegű adatok meghamisítása, és jogi eljárásokkal kapcsolatos megtévesztés;
- 6472. adatok megváltoztatása, és számítógépes szabotázs;
- 6780. adatok kikémlelése;
- 7151. szoftver – kalózkodás. Ez utóbbi 1991. óta szerepel.[88]

5. 2. Az informatikai bűncselekmények közös ismérveinek meghatározására tett kísérletek

Minél sokszínűbbé válik a számítógépes bűncselekmények köre, annál nehezebbé, nehézkesebbé válik a számítógépes bűncselekmények közös ismérveinek definiálása.

---

[87] Revue ... p(s). 472-473.
[88] Revue ... p(s). 322-323.

Az **OECD munkabizottsága** tanulmányában a cselekmények tipizálása mellett, összefoglalóan számítógépes visszaélésnek tekint minden olyan etikátlan, és jogtalan tevékenységet, amelyet az elektronikus adatfeldolgozási- és adatátviteli folyamat során követtek el.[89]

Az **ET. Szakbizottsága** megállapítja, hogy nem minden "etikátlan és jogtalan" cselekmény éri el a kriminalizáció szintjét, így ez a számítógépes bűncselekmény fogalmának kialakítására alkalmatlan. A bizottság emellett felrója azt is, hogy e meghatározásba nem fér bele az elektronikus adatfeldolgozási rendszerbe történő jogosulatlan behatolás. A bizottság áttekintve a korábbi években alkotott definíciók megállapításait, arra az álláspontra helyezkedik, hogy nem lehet egy rövid, tömör definícióban összefoglalni ezen bűncselekmények közös ismérveit.[90]

A spanyol **De La Torre** és **Frances** szerzőpáros szerint sem ragadható meg egy fogalomban a számítógépes bűncselekmények lényege heterogenitásük miatt. Hiszen ezek a támadások nemcsak a számítógépes rendszer ellen irányul, hanem más jogi értékek (így a privacy, az államtitok, valamint a közbizalom stb.) elleni támadásokat is magukba foglalják.[91]

E szerzőknél a *negatív* meghatározás indoka a veszélyeztetett jogtárgyak sokrétűsége.

De éppen a számítógépes információ tartalmának bővülése más szerzőket arra ösztönöz, hogy bizonyos kritériumokat fogalmazzon meg az elektronikus adatfeldolgozási rendszerek, és az ott kezelt információk elleni támadásokra vonatkozóan.

A **holland** törvényhozást segítő **Jogi Tanácsadó Testület** 1987-ből származó jelentésében megjelöli azokat az értékeket, amelyeket a büntetőjogi kódifikáció során feltétlenül érvényesíteni szükséges. In concreto a számítástechnikai adatok és eszközök elérhetősége, sérthetetlensége és kizárólagossága.[92]

---

[89] CE Recommendation (89) 9. ..... p(s). 10-11.
[90] Revue ... p. 13.
[91] Preliminary/Draft Versions for the use of the participants of the Computer Crime Conferences in Würzburg. Würzburg 1992. p(s). 300-301.
[92] Revue ... p. 472.

A 90-es évek elején a német **Ulrich Sieber** azon a véleményen van, hogy meg kell erősíteni egyfelől az információ birtokosának büntetőjogi védelmét. Ezen a területen egyrészt biztosítani kell az információ kizárólagos használatát, az üzleti titkok, és az intellektuális vagyoni jogok valamint más különleges státuszok védelmét. Másrészt biztosítani kell az adatok és információk integritását, helyességét, oszthatatlanságát és pontosságát. Másfelől a büntetőjognak garantálni kell az adatalany (akiről az információ szól) személyiségi védelmét (privacy) is. Fel kell lépnie az anyagi, és alaki privacy megsértőjével, az adatok használati jogának megszegőivel. Továbbá azzal szemben, aki a biztonsági intézkedéseket elhanyagolja. Véleménye az, hogy az információ felől ragadható meg a számítógépes környezetben elkövetett bűncselekmények közös ismérveinek meghatározása.[93]

Legújabban a görög **Irini Vassiliki** már multimédia - bűnözésről értekezik. Véleményét arra alapozza, hogy "egyre inkább az információs technikákkal való visszaélésről, valamint az adatok jogellenes használatáról van szó, amely a klasszikus számítógépes bűnözés szerkezetétől függetlenül alakult ki".[94]

---

[93] Revue ... p. 321. és vö. Sieber: The International Emergence ..... p(s). 35-39.
[94] Irini E. Vassiliki: Multimediale Kriminalität.Computer und Recht 13. 1997. 5. s. 297.

6. AZ INFORMATIKAI BŰNCSELEKMÉNYEK TÍPUSAI

Napjainkban a számítógépes környezetben elkövetett bűncselekmények az elektronikus adatfeldolgozás terjedésével, az információ-technológia és -kommunikáció fejlődésével egyre többféle jogsértés, illetve már szabályozott bűncselekmény elkövetésének a lehetősége.

A hálózatok megjelenésével, a számítógépek kommunikációjának általánossá válásával bővül az informatikai bűncselekmények elkövetésének tere, és repertoárja. A hálózatok multifunkcionálisak, azaz nemcsak elektronikus kereskedelmi ügyletek kötésére, tele(táv)-munka végzésére, telebank szolgáltatásra, hanem adatállományokhoz való hozzáférésre, üzenetek fogadására, továbbítására is képesek. Mind az egyes számítógép, mint egyes számítógépen keresztül bármely hálózat a számítógépes környezetben elkövethető bűncselekmény *eszköze,* illetőleg *célja.*

Eszköz, mivel az elkövetők a hálózaton keresztül férnek hozzá adatállományokhoz, azok megismerésének, módosításának szándékával, valamint átmenő adatok lehallgatása végett stb.

A hálózaton történő elkövetés, mint cél pl. a gyűlöletkeltő, az uszító (rasszista, antiszemita), továbbá a pornográf vagy a kábítószert népszerűsítő adatállományok létrehozása. Ezen túlmenően más bűncselekmények elkövetésére is alkalmas a világháló pl. az itt zajló elektronikus kereskedelem megzavarása a szerződések szövegének kifürkészését követően azt (pl. az aláírást, szöveget) módosítják. Idetartozik az ügyfelek adatainak, bankszámla számainak jogosulatlan megszerzése.

Szintén az elektromos kereskedelmet zavarja meg egy hamis WEB-oldal elhelyezése, amely áruház vagy bank, brókercég honlapját színleli. A vevő az áru- vagy szolgáltatás rendelésével, pénzügyi tranzakcióival együtt közli bankkártyaszámát, és egyéb információt. Ezáltal az elkövetők könnyedén hozzájutnak egy jóhiszemű személy adataihoz. Ebben az esetben a világháló egyszerre eszköze és célja a bűncselekménynek.

A világhálón elkövethető egyedi cselekmény az e-mail címre küldött pusztító vírus, amelynek megnyitásával aktivizálódik a vírusprogram, és a felhasználó adatállományait, boot-szektort stb. törli.

Az informatikai bűncselekmények fókuszában az elektronikus adat áll, amely tehát egyszerre lehet ezen bűncselekmények eszköze és célja.

1. Az elektronikus adat, is lehet eszköze a bűncselekményeknek:

a. közvetlen eszköze az adatmanipulációknak, amelyeket

- haszonszerzés céljával (pl. számítógépes csalás, bankkártyával visszaélés, hamis WEB-oldal elhelyezése a világhálón):
- hamisítás szándékával;
- károkozás szándékával (pl. vírus-programok),
- szabotázs (pl. kommunkációs rendszerek működésének megzavarása)

szándékával követnek el.

b. Közvetett eszköze: gyűlöletkeltő-, pornográf vagy egyéb jogellenes adatállományok létrehozása, megjelenítése végett a világhálón stb.

2. Az elektronikus adat a bűncselekmény elkövetésének céljaként funkcionálhat:

- a személyes, a különleges személyes adatok, a közérdekű adatok, valamint a jogilag védett titkok, mint elektronikus adatfeldolgozásra rendelt adatok jogosulatlan kifürkészése, illetéktelen személy számára történő hozzáférhetővé tétele stb.
- az elektronikus kommunikáció (e-mail, e-kereskedelem) tiltott lehallgatása;
- szoftverrel visszaélések (a szerzői jog által védett programok illegális másolása, használata, tiltott kereskedelme stb.)

Sajátos jogsértés a jogosulatlan belépés számítógépes rendszerekbe (a hacking), mivel ez egyaránt lehet a fentiek "előcselekménye".

6. 1. A jogosulatlan belépés a számítógépes rendszerekbe (hacking)

Az elektronikus adatfeldolgozási- és adatátviteli rendszerek védettsége, biztonsága e tevékenységek zavartalan ellátásának első és legalapvetőbb

követelménye. Az ilyen rendszerekbe történő behatolással az elkövető a biztonsági mechanizmusokat játssza ki, ezáltal teremti meg a védett adatállományokhoz a hozzáférés lehetőségét.

A számítógépes rendszerekbe történő jogosulatlan behatolást a szakirodalom általánosan - az angol nyelvből kölcsönzött - *hacking* kifejezéssel jelöli. Az angolszász országokban a hacking cselekményét a "házi béke" megsértéseként fogják fel. [95]

Az "elektronikus betörés" az adatállomány kezelésére szolgáló számítógépen keresztül, tehát közvetlenül, avagy a technika fejlődése folytán a számítógépes, és a telekommunikációs hálózatok integrációja révén a számítógépeket összekötő telefon vagy elektronikus adatátviteli vonalakon (dataline) keresztül, tehát közvetetten történhet.

Közvetlen hozzáférésről beszélünk azokban az esetekben, amikor az "elektronikus betörő" az elektronikus adatfeldolgozáshoz térben közel (pl. munkahelyén) fér hozzá jogellenesen az adatállományokhoz.

A közvetett hozzáférés a számítógépeket összekötő telekommunikációs hálózaton át történik, tehát - térben - távoli adatállományok elérésére nyílik lehetőség.

Az első esetben lehetséges az, hogy az elkövető jogosult ugyan a számítógép használatára, de számára tiltott belépési kódot igyekszik megfejteni, és így belépni a rendszerbe. Avagy, ha az elkövető nem jogosult a számítógép használatára, és akár a jogosult kódjával, akár azt próbálgatva jut be a rendszerbe. Idetartozik az is, ha az elkövetővel többen használhatják ugyanazt a számítógépet, viszont az elkövető mások kódját felhasználva férkőzik illetéktelenül a védett adatállományhoz.

Az elektronikus adatbankokhoz való hozzáférési jogosultság két irányban vizsgálandó. Egyfelől a felhasználónak milyen adatállományok elérése engedélyezett. Másfelől az általa elérhető adatokkal milyen műveletet végezhet: olvashatja, megváltoztathatja az adatokat, más műveletet végezhet azokkal stb. Ennek tisztázása elsődleges annak eldöntéséhez, hogy jogosulatlan behatolásról van-e szó, vagy sem.

Az "elektronikus betörés" a számítógépes rendszernek közvetlen, és ezáltal az adatállomány közvetett veszélyeztetésének legkorábbi stádiuma. Ugyanis a védett adatbankokhoz való jogosulatlan hozzáférés következtében az adatokról tudomás szerezhető, azok részben vagy egészben megváltoztathatók, törölhetők, más adatokkal kiegészíthetők, az adatállomány átrendezhető, amelynek eredményeképpen az nem vagy másképp értelmezhető. Továbbá valós veszélyt jelenthet a számítógépes vírus elhelyezése.

Az "elektronikus betörés" jogi minősítése nem egyértelmű az európai országokban. Ennek a cselekménytípusnak a kriminalizálása kivételesnek tekinthető.

Az 1988-ban módosított **holland büntető törvénykönyv** 138. szakasza szerint:

"(1) Aki szándékosan és jogellenesen behatol olyan számítógépes rendszerbe vagy annak egyik egységébe, amelyben adatot tárolnak vagy feldolgoznak 10.000 guldenig terjedő pénzbüntetéssel vagy 6 hónapig terjedő szabadságvesztéssel büntetendő, ha cselekményével

a. a biztonsági rendszert megsérti,

b. a behatolás olyan technikai megoldással történt, mint hamis jel, hamis kód, hamis kapacitás.

(2) 25.000.- guldenig terjedő pénzbüntetéssel vagy 4 évig terjedő szabadságvesztéssel büntetendő, ha az elkövető maga vagy más számára másol, visz be adatokat, és ezzel jogosulatlan előnyt szerez.

(3) 25.000.- guldenig terjedő pénzbüntetéssel és 4 évig terjedő szabadságvesztéssel büntetendő, ha az elkövető telekommunikációs rendszeren keresztül hatol be, ha ezzel

a. az automatizált rendszer feldolgozó-kapacitását jogosulatlanul használja fel előnyszerzés céljából vagy

---

[95] CE Recommendation (89) 9. ..... p(s). 51.

b. harmadik személy számára hozzáférhetővé teszi az automatizált rendszert." [96]

Az "elektronikus betörés" további eseteit találjuk a 350.a. szakasz (2) bekezdésében. E bekezdésben az adatokban történő károkozás súlyosabban minősül, és büntetendő, ha az elkövető ilyen módon jut a rendszerben tárolt vagy feldolgozott adatokhoz. A büntetés ekkor 25.000 gulden vagy 4 évig terjedő szabadságvesztés.

A holland Btk. minősített eseteiben az "elektronikus betörés" által véghez vihető "célcselekményeket" találjuk.

A **finn büntető törvénykönyv** 1991-es módosítása lényegesen egyszerűbben szabályozza ezt a magatartást: *"Aki a számítógépet jogszerűen használó kódjával, más azonosító kóddal vagy egyéb módon a védelmi rendszert kijátszva behatol olyan számítógépes hálózatba vagy annak egyik egységébe, amelyben adatfeldolgozás, -tárolás vagy -átvitel folyik pénzbüntetéssel vagy 6 hónapig terjedő szabadságvesztéssel büntetendő."* [97]

Az elkövetési magatartások körülírása utal arra, hogy azok technikailag többféle módon valósíthatók meg.

Az elkövetői kör csak a közvetlen "elektronikus betörés" esetében vonható meg viszonylagos biztonsággal. A számítógépes rendszerbe "kívülről" - közvetett módon - történő behatolás elkövetője bárki lehet.

---

[96] www.minjust.nl:8080/C__ACTUAL/PERSBER/compcrim.htm, és

Revue ... p. 490. - mindkettő saját fordítás.

[97] Centenary of the Finnish Penal Code. International Research Colloquium (24-27. September 1990. University of Helsinki) Finnish Criminal Code Reform. Law texts and drafts p. 40.

(A 100 éves finn büntetőkódex tiszteletére a helsini egyetemen 1990. szeptemberében rendezett tudományos ülésre készült előterjesztés 40.l. - saját fordítás.)

Az **olasz** büntető törvénykönyv módosításában, amelyet 1993. december 30-án hirdetnek ki az "elektronikus betörés" rendkívül részletes szabályozását nyújtja.

"615.szakasz: Aki jogtalanul belép olyan biztonsági intézkedéssel védett informatikai vagy teleinformatikai rendszerbe, amellyel az elkövetőt kirekeszteni szándékoztak három évig terjedő szabadságvesztéssel büntetendő.
A büntetés egy évtől öt évig terjedő szabadságvesztés;
1./ ha a bűncselekményt közhivatalnok vagy közszolgálat megbízottja követi el, hatalommal visszaélés, hivatali vagy szolgálati kötelesség megszegése esetében továbbá jogtalan magánnyomozói tevékenység során vagy rendszeroperátori minőségben;
2./ ha az elkövető erőszakkal vagy felfegyverkezve követi el;
3./ ha a bűncselekmény folytán a fenti rendszerek megsemmisítése, megrongálása, működésének teljes vagy részleges megszakítása, illetőleg az ott tárolt adatok vagy programok megsemmisítése vagy megrongálása származik.
A büntetés három évtől nyolc évig terjedő szabadságvesztés, ha a fentebb meghatározott cselekményeket katonai érdekeltségű vagy a közrendet, közbiztonságot, egészségügyet, valamint a polgári védelmet érintő informatikai vagy, teleinformatikai rendszerekre követik el." [98]

Magyarországon még nem általános a számítógépes, és a telekommunikációs rendszerek integrációja. Ez a legközelebbi jövő szükségszerűsége. Az "elektronikus betörés" hazai jogi minősítésének kérdését azzal kell kezdenem, hogy jogosulatlan behatolás esetén az "elektronikus betörő" elsődlegesen a számítástechnikai rendszerek védettségét, titkosságát töri meg. Ez tekinthető a bűncselekmény jogi tárgyának.

---

[98] Leggi, decreti e ordinanze presidenziali (Gazzetta Ufficiale Della Republica Italia, serie gen. n. 305.) 30.12.1993. 5.l. továbbá www.usl4.tos.it/dp/isll/lex/cp__12.htm - saját fordítás.

A cselekmény társadalomra veszélyességét, tehát e rendszerek biztonságához fűződő érdek megsértése jelenti. A rendszerbe történő belépést követően nyílik meg az elkövető előtt az adatok korrektsége, helyessége megváltoztatásának lehetősége, ami azonban vagyoni viszonyokat, személyiségi jogokat, üzleti- és gazdasági titkokat is veszélyeztethet.

Mindezek alapján véleményem szerint indokolt lenne e tevékenység önálló bűncselekménnyé nyilvánítása *szubszidiárius* jelleggel. Vagyis az "elektronikus betörő" csak akkor lenne felelősségre vonható, ha tevékenységével más - a későbbiekben részletezett - büntetendő cselekményt nem követ el.

A jogosulatlan belépés, mint bűncselekmény - súlyosságát tekintve - a vétségi alakzatot nem lépné túl.

6. 2. A számítógépes hamisítás

A modern technika fejlődésével a számítógép, és más számítástechnikai eszközök segítségével megvalósítható hamisítások a bűnözés új dimenzióját jelzik.

E cselekmények legnagyobb veszélye az, hogy a másolatok igen élethűek, így a hamis pénz nemcsak az utca emberét, hanem a pénzzel naponta dolgozókat is könnyen megtéveszti. A hamis vagy hamisított bankkártyákkal jelentős vagyoni károk okozhatók. A hamisított okiratok hatósági eljárásban használhatatlanok, és folytathatnánk a sort.

Kertész Imre szkeptikusan meg is jegyzi, hogy a mesterséges képalkotás, és a számítógépes grafika "nem fog ... sok örömet okozni a kriminalistáknak".[99]

Mivel a hamisítás nem valamennyi esetére terjed ki a büntetőjogi felelősségre vonás lehetősége, ezért a kriminalizáció kiterjesztése szükségesnek mutatkozik.

A számítógéppel végrehajtott hamisítások veszélyességére, valamint annak kriminalizálására először a **Gazdasági Együttműködési és Fejlesztési Szervezet** (OECD) munkabizottsága által készített elemzés hívja fel a figyelmet 1986-ban. E

---

[99] Dr. Kertész Imre: Kép- és hangtechnikai eszközök a büntetőeljárásban. Emlékkönyv Dr. Cséka Ervin születésének 70. és oktatói munkásságának 25. évfordulójára.(Szerkesztette: Tóth Károly.) Szeged, 1992. 324.l.

szerint számítógépes hamisításról beszélünk akkor, ha az adatok vagy programok bevitele, módosítása, törlése vagy elrejtése hamisítás céljából történik.[100]

Az **Európa Tanács** (89) 9. sz. Ajánlásában számítógépes hamisításként definiálják az elektronikus adatfeldolgozási folyamat befolyásolását adatok, és programok bevitelével, megváltoztatásával, törlésével, mentésével vagy más olyan beavatkozás által, amelynek eredménye az, hogy az elkövető magatartása a nemzeti büntetőjog által szabályozott hamisítás tényállásának megfelel.[101]

Nem véletlen, hogy az ET. ajánlását néhány évvel követő, a kilencvenes évek elején készült **Egyesült Nemzetek Szervezete** által kiadott kézikönyv számítógépes hamisításnak tekinti egyfelől azt, ha azzal a számítógépben tárolt adatok közokirati jellegét jogosulatlanul megváltoztatják, másfelől azokat az eseteket is, amikor a számítógépet a hamisítás eszközeként használják.[102]

Kertész Imre a számítógépes hamisítások körét az alábbiakban vonta meg:

a. az adatállomány meghamisítása (jogtalan megváltoztatása, törlése),

b. hamis kódkártya készítése és használata,

c. hamis bankjegy, okiratkészítését.[103]

Végső soron valamennyi esetben az adatok, információk megváltoztatása megelőzi a külvilágban is érzékelhető hamisítását. A számítógép memóriájában tárolt vagy bevitt (in-put) adatok meghamisítása azt a célt szolgálja, hogy ezen adatokat majdan valamely számítógépes rendszer működtetéséhez szükséges kártyák manipulálásának, továbbá okirat- illetve bankjegyhamisításához használják fel. Ebből következően e körből kiesnek az "egyszerű" fénymásolatok.

A jogalkotás és a jogalkalmazás szempontjait szem előtt tartva számítógépes hamisítás körébe tartozónak vélem:

1. a telefonkártyák hamisítását,

2. a bankkártyák és más ügyfélkártyák hamisítását,

---

[100] OECD - Analysis ... p. 9.
[101] OECD - Analysis ... p. 9.
[102] UN Draft ... p. 27.

3. a bankjegyhamisítást,

4. a közokiratok hamisítását.

A számítógéppel történő hamisítás alapja a számítógép memóriájában vagy valamely adathordozón (hajlékony- illetve kompaktlemezen, mágnesszalagon stb.) tárolt adatállomány jogtalan megváltoztatása, amely többféle módon lehetséges. Idevonható a program megváltoztatása, adatok törlése, téves vagy hiányos adatok betáplálása, továbbá bármilyen más olyan tevékenység, amely alkalmas arra, hogy az elektronikus adatfeldolgozás eredményét befolyásolja. A számítógépes hamisítás elkövetési magatartásai hasonlóak a számítógépes csaláséhoz. A két cselekmény abban különbözik egymástól, hogy az előbbi esetben a megváltoztatott adatokat dokumentumok készítéséhez fogják felhasználni, míg az utóbbi esetben az elektronikus adatfeldolgozás eredményének befolyásolása a cél, amelynek eredménye jogtalan vagyoni haszonszerzés vagy károkozás.

1. A *telefonkártyák hamisításának* "hőskorát" jelentette a kártyába épített chipnek (az ún. "törlőlábnak") leragasztása, ami megakadályozta kártya egységeinek fogyását, így ingyenesen telefonálhatott tovább a jogosulatlan használó. Ma már a high-tech bűnözők a telefonkártyán található chip információállományát manipulálják, programozzák át a számítógép segítségével. A kártyán levő IC-t a többszörösére tölthető fel (ma akár az ezerszeresére is növelhető az IC-n levő egység), vagy az IC-n levő egység újratölthető.

A telefonrendszer üzemeltetői, és a kártyahamisítók közötti kemény küzdelemben úgy tűnik, hogy nem az előbbiek állnak jobban. Ennek egyik oka az, hogy szakemberek szerint 1991-ben, bár korszerű, ám eléggé sebezhető telefonrendszert telepítenek Magyarországon.[104] A védekezés jelenlegi bizonytalanságát jelzi, hogy telefonkártyával az emeltdíjas telefonszámok, valamint néhány távol-keleti és arab ország nem hívható.

---

[103] Dr. Kertész Imre: A számítógépes hamisítás. RSz. XXI. 1993. 4. 14.l.

[104] adja hírül a Figyelő plusz - Tantusz, 1994. július 28. XVIII. lap

A bekövetkezett kárhoz viszonyítva, időben kissé késedelmes egy-egy új szoftver megjelenése. A piaci viszonyokból következik, hogy az ügyfelek fizetik meg a nem biztonságos rendszer működésének veszteségeit.

A rádiótelefonok megjelenését követte azok "klónozása", többszörözése. Azaz annak a chipnek a hamisítását, az "átégetését", amely a készülék tulajdonosa által sem ismert titkos elektronikus sorozatszámot (angolul: SEN-code) rejti. Ez az analóg mobiltelefonoknál valósítható meg, amelyeknél maga a készülék tartalmazza az alapadatokat, és nem válik el a szolgáltatás lehetősége külön a készülékre és külön a (SIM-) kártyára.

A chip hamisításához nélkülözhetetlen a már kiadott telefonszámok ismerete, amely a telefontársaságtól szerezhető meg belső informátortól, vagy a számítógépes adatbázisuk megcsapolásával.

A "klónozás" elvégzéséhez speciális szoftver szükségeltetik, amelynek készítése magas szintű programozói tudást tételez fel. Emellett, esetleg ennek hiányában a telefontársaságtól szerzett szoftver szükséges. A hamisítás révén az eredeti telefonszám tulajdonosát terheli a "klónozott" mobilon lebonyolított hívás is.

A hamis telefonkártyák készítése a Btk. 300/C. §-a szerinti számítógépes csalásként értékelhető, felhasználásuk, és a mobiltelefonok "klónozása" a (3) bekezdése szerint minősül.

A hatályos szabályozás szerint telefonkártyával való visszaélés első (annak készítése), és utolsó fázisa (felhasználása) büntetendő. A két szakasz közötti magatartások, így a hamisított telefonkártyák megszerzése, birtoklása nem büntethetők. Jóllehet e fázisok kapcsolódnak egymáshoz, összefüggnek egymással. Be kell látnunk, hogy a szabályozás eltúlzottan megnehezíti a rendőrség munkáját. Ugyanis ahogy a telefonkártya hamisítása, "végtelenítése" nem cél nélküli tevékenység, úgy annak bármilyen módon történő megszerzése, birtoklása sem az. E cselekménysorozatok a használatot megelőző aktusok. A hamisított telefonkártyákat felhasználás végett készítik, szerzik meg, illetőleg birtokolják.

Ez teremtheti meg annak elvi alapját, hogy ne csak a hamisított telefonkártyával történő visszaélés kezdő- és végső fázisát, hanem e szakaszokat összekötő

magatartásokat is kriminalizálni kellene egy önálló tényállásban, kiemelve azt a számítógépes csalás esetei közül. De lege ferenda úgy vélem: *"Aki közcélú távbeszélő szolgáltatás, illetve közcélú mobil rádiótelefon szolgáltatás igénybevételére szolgáló elektronikus kártyát készít, megszerez, birtokol illetőleg felhasznál, és ezzel kisebb kárt okoz vétséget követ el két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő."*

2./ A *bankkártyák, és más ügyfélkártyák hamisítása* is a high-tech bűnözés új "üzletága". A bankkártyák többféle bűncselekmény tevékenységi tárgyai lehetnek. Ehelyütt a hamisítás kérdésével foglalkozom.

A hamisítások tipikus célpontja a bankkártya hátoldalán levő mágnescsík. Mivel ez megegyezik a videokazetták szalagszélességével, így bárki rendelkezésére áll egy előmágnesezett csík. Erre felvihető a kártyáról egyelőre csak "magán-importból" beszerezhető kártyaleolvasó-géppel szerzett adatok és ezzel akár a lopott kártyák adatai is felülírhatók, akár az eredeti kártyák "ikertestvérei" is előállíthatók. Ritkábban a kártya felületén dombornyomással készült számkombináció hamisítására is vetemednek az elkövetők. Azt kivasalják, majd más számok nyomnak rá. A cselekmény eddig a pontig a bankkártya-hamisítás tilalmát rögzítő Btk. 313/B. § (1) bekezdés a. pontjába ütközik.

A nemzetközi joggyakorlatban a több büntető törvénykönyvben is találunk kártyahamisítás körébe tartozó bűncselekményt. A **német** jogban büntetni rendelik az eurocsekk és eurocsekk-kártya hamisítást (StGB 152.a §). Ez felöli akár a külföldi, akár a belföldi eurocsekk- és kártya meghamisítását, illetőleg hamisított változatuk felhasználását. A **svájci** Btk.-ban a csekk- és a hitelkártya-hamisítást a 148. §-ban találjuk.[105] A **magyar** Btk. a 313/B. §-ában rendeli büntetni bankkártya - hamisítást:

313/B. § (1) Aki felhasználás céljából

a./ bankkártyát meghamisít vagy hamis bankkártyát készít,

---

[105] www.gesetze.ch/sr/311.0/311.0_012.htm

b./ hamis vagy meghamisított bankkártyát megszerez, ha súlyosabb bűncselekmény nem valósul meg, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő az is, aki a bankkártya-hamisítást a csekkgarantáló kártyához tartozó csekkre nézve követi el.

(3) Aki bankkártya - hamisításra irányuló előkészületet követ el, vétség miatt pénzbüntetéssel büntetendő.

"Aki felhasználás céljából

a./ bankkártyát meghamisít vagy hamis bankkártyát készít,

b./ hamis vagy meghamisított bankkártyát megszerez, ha súlyosabb bűncselekmény nem valósul meg, vétségét követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő az is, aki a bankkártya-hamisítást a csekkgarantáló kártyához tartozó csekkre nézve követi el.

(3) Aki bankkártya - hamisításra irányuló előkészületet követ el, vétség miatt pénzbüntetéssel büntetendő.

E bűncselekmény jogi tárgya közvetve a bankkártya-forgalom biztonsága, közvetlenül pedig a bankkártyákba vetett bizalom.

Elkövetési tárgynak a Btk. 313/D. §-ban meghatározott kártyákat tekintjük, azaz „minden olyan, pénzintézeti tevékenységet végző jogi személy által kibocsátott kártya, amely pénz felvételére, illetőleg áru vagy szolgáltatás ellenértékének kiegyenlítésére szolgál."

Az elkövetési magatartás a bankkártya meghamisítása, amely felöleli azokat falzifikáló ténykedéseket, amikor egy már létező bankkártyát, illetőleg az azon található információkat változtatják meg. E magatartásnak a technikai megoldása közömbös.

Hamis bankkártya készítése esetében egy korábban nem létezett bankkártya jön létre, pl. "nyers" kártyát látnak el a szükséges információkkal vagy egy már létező

---

[105] www.gesetze.ch/sr/311.0/311.0_012.htm

bankkártyát megtöbbszöröznek stb. Nemcsak hamisítás technikája, hanem minősége is közömbös.

Az alanyi elemek értékelésekor arra kell felhívni a figyelmet, hogy a bankkártya hamisításnak célzatosnak kell lennie, és e célzat a bankkártya felhasználása. Irányadó e körben is, hogy a célzatos deliktum csak egyenes szándékkal valósítható meg.

Egyébiránt a bűncselekmény befejezettségéhez a bankkártya tényleges felhasználásának nem kell megtörténnie.

A bankkártya-hamisítás akkor minősíthető e törvényhely alapján, ha súlyosabb bűncselekmény nem valósul meg. Utóbbiként a csalás (Btk. 318. §) jöhet szóba.

A delictum sui generis előkészületi cselekményeknek az a specialitása, hogy a törvényhozó önmagában előkészületi cselekményt befejezett bűncselekményként értékel, amelynek aztán így szintén megállapítható kísérlete stb.

A bankkártya-hamisítás, mint delictum sui generis előkészületnek az előkészülete büntetendő. Idetartozhat a hamisításhoz szükséges vagy ezt könnyítő feltételek, pl. technikai eszközök biztosítása, továbbá olyan verbális cselekmények, mint a bűncselekményre való felhívás, ajánlkozás, vállalkozás, s közös elkövetésben való megállapodás.

Az előkészületi magatartásoknak célzatosnak kell lennie és ez bankkártya hamisítás felhasználás végett való előállítása.

Amennyiben az elkövető a bankkártyát fel is használja jogtalan pénzszerzés céljából, akkor a 313/C. §-ban meghatározott bankkártyával visszaélés bűncselekményét követi el. A cselekmény minősítése és a büntetési tételek az okozott kár mértékétől függ.

3./ A *bankjegyhamisítás* kapcsán **Karl Binding** német jogtudós a századfordulón nem kevés malíciával azt írja, hogy a pénz feltalálása egyidejűleg a pénzhamisítás feltalálásához is vezetett.[106]

A pénzhamisítás első részletes szabályait a római Sulla fekteti le i.e. 80-ban. Törvényében a lex Cornelia de falsis-ban bünteti a hamis pénz forgalomba hozatalát, a forgalomban levő pénz utánzását stb.[107] Ezt követően a pénzhamisítás relatív állandósággal jelen van a büntető törvénykönyvekben, bár az elkövetési magatartások köre és persze technikai megoldásai szélesednek, tökéletesednek.

Ma a nyomdák papírpénz nyomásához különleges gyapotból készült papírt használnak. E papírok minőségét, és ezzel felhasználhatóságát megállapító alapanyag különböző komponenseiből következtethetünk annak korára, ami a hamisítás megállapításához nélkülözhetetlen információ. (Egy - egy példa, kizárólag a régmúltból: titániumot az 1930. után, optikai fehérítőt az 1950. után készült papírokban találhatunk, műszálas papírt 1960. óta gyártanak stb.)
A papírpénzekbe számos biztonsági elemet építenek be, amelyek a hamisítást megnehezítik vagy kizárják. A xerox által észrevehetetlen vízjelképpel vagy vízjelmezővel, teljes vagy "ablakos" fémszállal vagy újabban hologram hatású fémcsíkkal, vonalkóddal, mikroírással, rejtett képpel vagy felirattal, ún. illeszkedőjellel, különleges fénynél fluoreszkáló rajzolattal, számsorral, jelzőrostokkal stb. látják el azokat, a nyomtatása során többféle (sík-, magas- illetőleg metszetnyomtatási eljárást) alkalmaznak egy ugyanazon bankjegy előállításakor. Ezenfelül a könnyedén kikeverhető standard színek helyett mixelt színeket használnak, ráadásul adott helyen megnövelt festékvastagsággal. A metszett, apró részletekbe hajló arcképpel, és hátoldali képpel nemcsak szebbé teszik a pénzt, hanem a hamisítóknak is feladják a leckét. De egyéb "ravaszsággal" is igyekeznek gátat szabni a hamisításoknak: a német márkán fellelhetünk ún. átnézőjelet, amely a fény felé

---

[106] Karl Binding: Lehrbuch des Deutsches Straftrecht II. München und Leipzig 1904. s. 306.
[107] Dr. Zlinszky János: A római büntetőjog, Miskolc 1992. 135.l.

fordítva egy "D" betűt mutat, ugyancsak a német márka csak rézsutosan azonosítható, "olvasható le", és erre a képolvasók képtelenek.[108] Ma még...

A számítógéppel végrehajtott pénz- és okirathamisítás elkövetéséhez szükség van egy képolvasóra vagy egy ún. fotó CD-re, számítógépre, grafikai programra és lézernyomtatóra. A képolvasó az általa leolvasott képet digitális jelekké alakítja át, és azt továbbítja a számítógép memóriaegységébe, ahol egy grafikai program segítségével a szöveget, és a képet alkotó jeleket meg lehet kiegészíteni, módosítani, majd a megváltoztatott kép kinyomtatása következik.

A pénzforgalom biztonságát veszélyeztető hamisítás ellen a nemzeti bankok a pénz bevonásával válaszolnak (vagy inkább erre kényszerülnek). Nagy-Britanniában 1945-ben vonják be a 10 fontnál nagyobb névértékű bankjegyeket, mivel a náci Németország jó minőségű angol bankjegyekkel kívánja elárasztani a piacot. Magyarországon 1925-ben pattan ki a frank - hamisítás néven elhíresült ügy. Vezető magyar politikusok tudtával és beleegyezésével hamis frankokat nyomnak a fővárosi Térképészeti Intézetben. A hamis bankjegykötegeket a sárospataki vár pincéiben tárolják. A hamis pénzt valódi pénzzé átmosva kívánják legalizálni, de Hágában lebuknak a magyar ügynökök. Az eset erkölcsi tanulságaként citáljuk **Károlyi Mihályt.** Emlékirataiban azt írja, hogy "az ügy igazi érdekessége....., hogy a botrányba a legfelsőbb körök, és a kormányzat képviselői is belekeveredtek, és ezt senki sem tartotta szégyenletesnek."[109]

Hazánkban 1999-ben a Magyar Nemzeti Bank néhány hét alatt bevonja az akkor érvényes 5.000.- ft-os papírpénzt, mivel megtévesztően jó minőségű másolatok kerülnek forgalomba.

A **magyar** büntetőtörvénykönyv az alábbiak szerint rendeli büntetni a pénzhamisítást:

304. § (1) Aki

---

[108] Bankjegyismeret (Kiadja: MNB. Belső használatra). Budapest, 1998. 5-17.l.
[109] Károlyi Mihály: Hit, illuziók nélkül. Budapest 1977. 103.l.

a./ forgalomban levő pénzt forgalomba hozatal céljából utánoz vagy meghamisít,
b./ hamis vagy meghamisított pénzt forgalombahozatal céljából megszerez,
c./ hamis vagy meghamisított pénzt forgalomba hoz
bűntettet követ el, és két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.
(2) A büntetés öt évtől tíz évig terjedő szabadságvesztés, ha a pénzhamisítást
a./ bűnszövetségben,
b./ nagy mennyiségű vagy értékű pénzre követik el.
(3) A büntetés öt évig terjedő szabadságvesztés, ha a hamisítás tárgya váltópénz vagy ha a hamis vagy meghamisított pénz mennyisége vagy értéke nem jelentős.
(4) Aki pénzhamisításra irányuló előkészületet követ el, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.
305. § A 304. § alkalmazása szempontjából
a./ forgalomban levő pénz utánzásának kell tekinteni a forgalomból kivont pénz olyan megváltoztatását is, hogy az forgalomban levő pénz látszatát keltse,
b./ pénz meghamisításának kell tekinteni olyan jelzés alkalmazását, illetve eltávolítását is, amely annak megjelölésére szolgál, hogy a pénz csak meghatározott országban érvényes, továbbá a pénz nemesfémtartalmának csökkentését is.

A büntető törvénykönyvet életbeléptető Btké. 24. §-a kiegészíti a bűncselekmény tevékenységi tárgyainak sorát. A büntetőjog alkalmazása szempontjából papírpénznek tekinti az állam által kibocsátott értékpapírt, a kötvényt, a letéti jegyet, a befektetési jegyet, a részvényt, a vagyonjegyet, a csekket, és az utazási csekket, feltéve, hogy a névre szóló értékpapír átruházását jogszabály vagy az értékpapíron feltüntetett nyilatkozat nem zárja ki vagy nem korlátozza. Továbbá a külföldi pénz, és értékpapír ugyanolyan védelemben részesül, mint a magyar fizetőeszköz.

A bűncselekmény tárgyi oldalán az alábbi elkövetési magatartásokat találjuk: *a.* forgalomban levő pénznek forgalomba hozatal céljából történő utánzása vagy meghamisítása. A pénzutánzás esetében az elkövető forgalomban levő pénz hasonmását igyekszik létrehozni. Egyszerű módszerként használják valamely

papírpénz színes nyomtatón való másolását. Ezzel a kissé primitív eljárással viszont nem utánozhatók még bankjegypapíron sem a metszet-mélynyomtatással készült pl. portré, hátoldali kép és más díszítő elemek.

A másológépek (egyelőre) nem képesek a papírpénzen szereplő egy-egy portré finom vonalainak, valamint színátmeneteinek a reprodukálására.

A pénzhamisítás lényegesen fejlettebb módszere az, ha számítógépen történő tervezéssel a klisé házilagos előállítását követően azt nyomdában teszik valódi bankjegypapírra. Viszont valódi klisé hiányában a biztonsági elemek valójában nem pótolhatók.

A cselekmény büntetőjogi megítélése szempontjából nem az a lényeges, hogy a pénzutánzás hogyan sikerült, milyen minőségű, hanem az, hogy az elkövető arra törekedett-e, hogy más tárgyból pénzt állítson elő, pénzként felhasználás végett.[110]

A hazai bírói gyakorlatban a valódi pénzről egyszerű xerox (fekete-fehér) másolat is hamis pénznek tekintendő.[111]

Ugyanígy pénzhamisítás az 500 forintos bankjegyről fénymásoló gépen történő másolás.[112]

Az alapesetben értékelt egyéb elkövetési magatartások:

b. hamis vagy meghamisított pénz forgalomba hozatal céljából történő megszerzése,

c. hamis vagy meghamisított pénz forgalomba hozása (pl. átadása, ajándékozása, más számára való hozzáférhetővé tétele) tanúsításához nem szükséges számítógép.

A (2) bekezdésben szereplő:

a. bűnszövetség akkor valósul meg, ha az elkövető ugyanolyan vagy hasonló bűncselekmény elkövetésével anyagi haszonszerzésre törekszik.

b. A nagy mennyiségű vagy értékű pénz megállapítását a bírói gyakorlatra bízza a jogalkotó. Irányadó lehet az a döntés, amely a hamis bankjegyek szélesebb körben

---

[110] BH. 1986/312.
[111] BH. 1984/482. és 1989/346.
[112] BH. 1988/391.

való elterjedésének veszélyét, mint értékelni kívánt körülményre hívja fel a figyelmet.[113]

A (3) bekezdésben említett privilegizált eset megítélése szintén a bírói gyakorlatra marad. Nyilvánvalóan itt is a hamis bankjegyek, érmék darabszáma, értéke, elterjedésének veszélye stb. igényel értékelést.

A bűncselekmény tárgyi súlyára tekintettel a törvényhozó az előkészületet is kriminalizálja. "Ha a törvény külön elrendeli előkészület miatt büntetendő, aki a bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő feltételeket biztosítja, továbbá az elkövetésre felhív, ajánlkozik, vállalkozik vagy közös elkövetésben megállapodik" (Btk. 18. §).

A materiális előkészületi magatartások közül különösen a pénzhamisításhoz szükséges speciális technikai eszközök (képolvasó, grafikai programok, nyomtatók vagy más nyomdai berendezések) beszerzése előkészületként értékelhető, feltéve, ha erre a pénzhamisítás megvalósításának céljából kerül sor.

Tekintettel az egyre fejlettebb hamisítási eljárások térnyerésére, nélkülözhetetlen az állampolgárok megismertetése a biztonsági megoldásokkal azért, hogy különbséget tudjanak tenni a hamis illetőleg a valódi pénz között. Nem elégséges az a jó szándékú törekvés, hogy - az új bankjegyek megjelenése előtt - a Magyar Nemzeti Bank tájékoztatóit postahivatalokban, pénzintézetekben terjeszti.

4. A számítógépek nagy tömegű és gyors adatkezelésének előnyei a közigazgatási területén is elvitathatatlan. Viszont az adatváltoztatás *számítógépben vagy más adathordozón tárolt közokirat készítéséhez felhasznált adatok hamisításának* veszélyére fel kell figyelnünk.

Azzal, hogy egyes képelemek külön-külön kiemelhetők, lehetővé vált a teljes kép vagy egy részének megváltoztatása pl. személyek, tárgyak, számok, betűk, egyéb jelek (pecsét) eltüntethetők a képről, iratról, papírpénzről, illetve azok egyben ki is egészíthetők.

---

[113] BH. 1986/360.

Az adatok tartalmának sokrétűsége miatt nemcsak vagyoni értékeket jelölhetnek, hanem állami - társadalmi - gazdasági - jogi - igazgatási kapcsolatokat megalapozó tényeket is, amelyek valódiságukkal megalapozzák, igazolják e viszonyok létezését, funkcionálását vagy megszűntét. Az elektronikus adatfeldolgozás keretében ezen adatokat ugyanúgy közhitelesnek kell tekintenünk, mint a papíron rögzített közokirat esetében.

A közhitelesség, mint kiemelkedő érték, és érdek védelmére az állam büntetőjogi eszközöket is igénybe vesz. Az eddigi jogfejlődés során a közhitelességen alapuló közbizalom (publica fides) büntetőjogi védelme akkor jött, és jön szóba, ha az adatok, tények, nyilatkozatok, intézkedések illetve határozatok köz- vagy magánokirat formájában öltenek testet. A magyar jogtörténetben a hamisítás körébe tartozó, az 1462:II. törvénnyel bevezetett, majd többször (pl. 1495: IV. törvénnyel is) módosított hűtlenség körében szabályozott - mára teljesen elfeledett fogalmat felelevenítve - ún. állevélkötés.[114]

Ma az okiratok kiállítása történhet a számítógépben tárolt adatok alapján, azok lekérdezésével, vagy azáltal, hogy maga a számítógép egy utasítást (pl. billentyű megnyomását) követően állít elő ilyen okiratokat, akár úgy, hogy azokat a hozzá kapcsolt printeren kinyomtatja, akár úgy, hogy programja egy blanquetta kitöltését vezérli.

Napjainkban az adatok manipulásával vagy az elektronikus adatfeldolgozás egyéb módon történő jogosulatlan befolyásolásával létrejövő adatok a közhitelességbe vetett bizalmat rendítik meg azáltal, hogy annak bizonyítására alkalmatlanná válnak.

A számítógép memóriájában vagy adathordozón tárolt adatok manipulálása ilyen bűncselekmények megvalósulásának a legkorábbi, a büntetőjogban előkészületként értékelendő szakaszát is jelentik.

A külföldi tapasztalatok azt mutatják, hogy egy sor ország eltérő módon ugyan, de üldözi a számítógépes hamisítás elkövetőit.

---

[114] Dr. Angyal Pál: Okirathamisítás. Bélyeghamisítás. Védjegybitorlás. Csalárd és vétkes bukás. (A magyar büntetőjog kézikönyve 5. kötet) Budapest, 1929. 6.l.

A. A büntetőjogi felelősség kialakításakor egyes országban új tényállást alkotnak, míg másutt kiterjesztő értelmezéssel élnek. Az előbbi körbe sorolható a **német** szabályozás. A számítógépes bűncselekményeket bevezető 1987-es módosítással büntetendővé nyilvánítják a számítógépes hamisítás meghatározott eseteit, amelyet a deliktum újdonsága miatt célszerű részletesebben áttekinteni:

"269. § Bizonyítási jelentőségű adatok meghamisítása
(1) Aki jogügyleti forgalomban megtévesztésül bizonyítási jelentőségű adatokat úgy tárol vagy változtat meg, hogy azok alkalmazása révén hamis vagy hamisított okirat jönne létre, vagy ilyen módon tárolt, valamint megváltoztatott adatokat használ öt évig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő.
(2) A kísérlet büntetendő."

A **német** Btk. az okirat-hamisításokat büntetni rendelő tényállások mellé helyezi a bizonyítási jelentőségű adatok meghamisítása bűncselekményt, jelezve azt, hogy ennek a tényállásnak kiegészítő funkciót szán.

Amíg az előbbi eleme a vizuálisan érzékelhető adatok, addig az utóbbié az elektronikus adatfeldolgozás során keletkezett és tárolt adatok. Ezek közül is csupán azok, amelyek bizonyítási jelentőségűek, vagyis amelyek adott jogviszony bizonyítására szolgálnak.

A bűncselekmény elkövetési magatartása az adatok megváltoztatása illetve ezek használata. Az adatváltoztatás elérhető az adatok vagy a programok szándékos manipulálásával. A fals adatok használata akkor jön szóba, ha azokat az adatfeldolgozás- és átvitel során szándékosan, tehát hamisságukat tudva alkalmazzák.[115]

---

[115] Dr. Eduard Dreher - Dr. Herbert Tröndle: Strafgesetzbuch und Nebengesetze. München 1993. s(n). 1618-1621.

Szintén 1988-ban a **japán** Btk.-t is módosítják, és büntetendővé nyilvánítják a számítógépes hamisítását. A szövegezés szokatlanul technicizált.

"161-2. § (1) Aki másra vonatkozó tényállás meghamisítása végett, jogellenesen előállít olyan elektromágneses jelet, amelyet igazgatási eljárásban használnak, továbbá olyan jog, kötelezettség létét vagy igazolást jelöl, amelyek tényállás alapjául szolgálnak 500.000 yenig terjedő pénzbüntetéssel vagy 5 évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés 1 millió yenig vagy 10 évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott cselekményt közhivatalban vagy közhivatalnok követi el.

(3) Aki a meghamisított elektro-mágneses jelet, amely jog, kötelezettség létének vagy igazolás jelölésére szolgál más személyt érintő tényállás kialakításához felhasznál az (1) bekezdésben meghatározott módon büntetendő.

(4) A kísérlet is büntetendő." [116]

A japán rendelkezés szerint a bűncselekmény akkor valósul meg, ha elkövetési tárgyként olyan adatot hamisítanak meg, amely igazgatási eljárásban tényállás kialakítására szolgál. Minősített eset és egyben súlyosabban büntetendő a közhivatalban vagy közhivatalnok által elkövetett adathamisítás.

A következő évben jelenik meg a **francia** Code Penal módosítása, amely a dokumentumok egy sajátos fajtájának meghamisítását rendeli büntetni.

"462-5. §: Aki hírközlési dokumentumokat meghamisít, ezek jellegétől és formájától függetlenül, és ezzel kárt okoz 20.000.- franktól 2.000.000.- frankig terjedő pénzbüntetéssel vagy egy évtől öt évig terjedő szabadságvesztéssel.

462-6. §: Aki ezen informatikai adatokat felhasznál a 462-5. § szerint 200.000.- franktól 2.000.000.- frankig terjedő pénzbüntetéssel vagy egy évtől öt évig terjedő szabadságvesztéssel büntetendő." [117]

---

[116] Revue ... p. 441.

B. A büntetőjogi felelősség megteremtésének másik módja az, hogy a tradicionális hamisítás bűncselekményének elkövetési tárgyát a törvény kiterjesztően értelmezi.

A **finn** büntető törvénykönyv 1992. évi centenáriumi módosítása legalizálja a korábbi bírói gyakorlatot. Egy 1985-ben született bírósági ítélet kiterjeszti a bizonyíték fogalmát a számítógépes adatokra.[118]

A módosító novella 33. fejezetének 1. § szabályozott hamisítás tényállása az adatok falzifikálása esetében is alkalmazandó. *"Aki hamis okiratot vagy bizonyítékot készít, vagy okiratot, bizonyítékot abból a célból hamisít meg, hogy ezeket a megtévesztésül használja, továbbá hamis vagy hamisított bizonyítékot felhasznál pénzbüntetéssel vagy két évig terjedő szabadságvesztéssel büntetendő.*
Az itt található értelmező rendelkezése megfogalmazza azt, hogy a bizonyítékként értékelhető az elektronikus adatfeldolgozásra alkalmas adatok.

A **görög** Btk.-ban egy értelmező rendelkezéssel szüntetik meg az esetlegesen keletkező jogbizonytalanságot. Ebben a dokumentum fogalmába felvették a bankkártyán, mágneslemezen, és szalagon szereplő, valamint a számítógép memóriájában őrzött adatot.[119]

Az **olasz** törvényhozás egy hivatkozó diszpozícióval, ennek részeként egy értelmező rendelkezéssel teszi egyértelmű az adat vagy program hamisításának büntetőjogi értékelését:
"491. § Informatikai magán- vagy közdokumentum meghamisítására vonatkozóan a köz- és a magánokirat-hamisítás rendelkezései alkalmazandók.
Informatikai dokumentumokon értendő az adatállomány, amely feldolgozásra szánt adatokat, bizonyító hatályú információkat vagy programokat tartalmaz." [120]

---

[117] Code Pénal. 1900-1991. (Cinquiéme Édition). Paris, 1990. p. 445. - saját fordítás.
[118] Revue ... p. 276.
[119] Revue ... p. 370.
[120] v.ö. 98.

A nemzetközi judikatúra részleges áttekintése is meggyőzhet arról, hogy **hazánkban** is szükségesnek mutatkozott a számítógépes adatok hamisításának büntetendővé nyilvánítása.

Az 1996. évi LII. tv. a közokirat-hamisítás előkészületének büntetni rendeltségét teremti meg. Nem kétséges, hogy előkészületi magatartásként értékelhető az adatmanipulálás is, amely nem más, mint a bűncselekmény elkövetéséhez szükséges feltételek biztosítása.

Magam az előkészületet de lege ferenda pontosítanám, konkretizálnám.

"(1) Aki az elektronikus adatfeldolgozás- vagy adatátvitel során olyan adatot, amely közokirat bizonyító erejéhez szükséges megváltoztat vagy használ vétséget követ el két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) Az a hivatalos személy, aki hivatali hatáskörével visszaélve követi el az (1) bekezdésben meghatározott cselekményt bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."

A bűncselekmény tevékenységi tárgyaként csak olyan adat szerepelne, amely a közokirat bizonyító erejéhez szükséges. Közokirat a magyar jogban olyan okirat, amelyet bíróság, közjegyző vagy más hatóság ügykörén belül a megszabott alakban állított ki, továbbá azon okiratok, amelyeket más jogszabály közokiratok közé emel (Pp. 195. § (1) bekezdés).

Ki kell emelni a de lege ferenda értelmezéséhez, hogy csak a számítógépben tárolt vagy bármilyen adathordozón rögzített adatok vehetők figyelembe.

A tényállás tárgyi oldalán levő tevékenységi magatartás a tárolt adatok meghamisítása, amely történhet akár az adatok, akár a program manipuláció eredményeképpen, és a már hamisított adatok használata pl. további adatfeldolgozás során vagy adatátvitelkor. Ez utóbbi csak akkor lenne büntethető, ha az elkövető tisztában van az adatok hamisságával és azzal, hogy ezeket az adatokat közokirat elkészítéséhez használhatják.

A de lege ferenda tényállás struktúrája követné a közokirat-hamisítás szerkezetét, vagyis súlyosabban minősülő és büntetendő lenne a hivatalos személy által hivatali hatáskörében elkövetett adathamisítás. Ez az elkövetési forma kínálkozik kézenfekvőnek. Azonban ne felejtsük el, hogy a számítógépes adatállományokhoz hamisítási szándékkal kívülről is hozzáférhetnek és manipulálhatók.

Amennyiben a számítógépbe történő hamis adatbevitelt (in - put fázist) követően azonnal kinyomtatásra kerül a közokirat, úgy a cselekmény a Btk. 274. § (1) bekezdésébe ütköző és minősülő közokirat-hamisítás bűncselekményének értékelhető.

A számítógéppel végrehajtható tökélyig /?/ véghezvihető hamisítás kapcsán felrémlik **George Orwell** negyvenes évek végén írott démoni látomása a dokumentumok meghamisításának veszélyességéről, amely természetesen túlmutat a büntetőjogi felelősség problémakörén: "Mihelyt..... szükségessé vált valamennyi javítást végrehajtották és ellenőrizték, a szóban forgó számot újranyomtatták, az eredeti példányt megsemmisítették, és a javított példányt tették a helyére. Ezt az állandó változtatási eljárást alkalmazták nemcsak az újságokban, hanem a könyvekben, folyóiratokban, pamfletekben, plakátokon, röpiratokban, filmeken, hanglemezeken, karikatúrákon és fényképeken is - azaz minden olyan irodalmi vagy ideológiai szempontból jelentősége lehetett. A múltat napról napra, sőt szinte percről percre a jelenhez igazították. ..... nem tűrték, hogy egyetlen olyan hírnek vagy kinyilatkoztatásnak nyoma maradjon, amely ellentétben volt a pillanatnyi követelményekkel."[121]

6. 3. A számítógépes csalás

A számítógépes környezetben végrehajtott első bűncselekmények a jogosulatlan haszonszerzés végett elkövetett manipulációk.

---

[121] George Orwell: 1984., Budapest, 1989. 47-48.l.

Az elektronikus adatfeldolgozási folyamatot vagy annak eredményét befolyásoló megtévesztő magatartások, mint számítógépes csalás elnevezéssel válik ismertté. A fondorlatok - talán végtelen - változatos formát ölthetnek.

A számítógépes csalások jellemzője az, hogy az elkövető magának vagy általa harmadik személynek jogosulatlan haszon megszerzése céljából, az adatot vagy a programot manipulálja.

Lássunk néhány klasszikussá vált elkövetési magatartást e körből.

1. Az elkövető helytelen vagy hiányos adatot táplál a számítógépbe, jogosulatlanul részben vagy egészben módosítja, törli, elrejti az adatokat, vagy más olyan beavatkozást hajt végre, amelynek eredményeként a számítógép:

1.a. Az elkövető vagy általa más személy számára fiktív számlát vagy folyószámlahitelt nyit. (A Stanley Mark Rifkin-eset szolgál erre például.)

1.b. Fiktív vagy valódi számlára jogtalan kifizetéseket eszközöl. A magyar OTP alkalmazottja egy külföldi ügyfél számlájára fiktív kamatot iratott jóvá.[122] Az akkori Német Szövetségi Köztársaságban egy programozó több kiskorú gyermek után járó családi pótlékot utaltatott át nagyanyjának, aki mellesleg 80. esztendős volt.[123]

1.c. Fiktív átutalásokat végez saját vagy harmadik személy számlájára. Az Amerikai Egyesült Államokban U.D. Savings Bank pénztárosa a pénzintézet inaktív számláiról saját számlájára utaltatott 290.000.- dollárt.[124] A japán Agricultural Coop alkalmazottja a cég komputere segítségével 48 millió yent utaltatott át bátyja bankszámlájára. [125]

---

[122] adja hírül a Computerworld - Számítástechnika 1988. 22. a 11. lapon

[123] Dr. Pusztai László: Komputerbűnözés és a büntetőjogi reform az NSZK-ban. MJ. 34. 1987.11.sz. 958.l.

[124] vö. A.N. Smith - W.J. Alexander - D.B. Medley... p. 402.

[125] Atsushi Yamaguchi: Computer - related Crime in Japán. Tokyo, 1992. (Kézirat a würzburgi konferenciára.) p. 5.

1.d. Az elkövetőnek vagy harmadik személynek az adósságát részben vagy egészben törli. Hazánkban az elkövető a számítógépterembe beosonva a 2.900.- ft-os vállalati lakbérhátralékát 3.000.- ft. bebillentyűzésével "egyenlítette ki".[126]
1.e. Jogszerű szolgáltatást vagy kifizetést megsokszoroz és minden bizonnyal folytathatnánk a sort.

Ilyen, és ehhez hasonló aktív magatartások mellett nagyon - nagyon ritkán *mulasztással* valósul meg a bűncselekmény. Az NSZK-ban egy programozó nem törölte a nyugdíjasok névsorából azok nevét, akik időközben elhunytak, hanem ezek nevére érkező járandóságokat a saját számlájára utalta.[127]

2. Az elkövetési magatartások másik fő típusa a számítógép programjának manipulálása. Az egyik müncheni bank dolgozója olyan programot szerkesztett, amelyben az aritmetikai utasítás a pénzösszeg tizedeire, a kifizetés pedig kerekített összegre vonatkozik. Az így keletkezett különbséget utalta saját számlájára. Ez az összeg nem elhanyagolható, hiszen fél év alatt kb. 500.000.- német márkát "gyűjtöget össze".[128] Egy bostoni bank alkalmazottja programjával minden betétes számlájáról "lecsípett" egy - egy centet, amit a névsorban szereplő utolsó betétes számlájára utalt át. Ugye, nem nehéz kitalálni kinek a nevére.[129] Egy minneapolisi bank részére egy "külsős" programozó, olyan programot szerkesztett, amely később az ő nevére szóló, de fedezetlen kártyáját is feldolgozta. "Ötletével" 135.733.- dollár kárt okozott.[130]

A programmanipuláció - szintén - kivételesen, de mulasztással is elérhető pl. ha a programozó programjából "kifelejti" az ún. ellenőrzési mechanizmusokat és ezzel teszi lehetővé bűncselekmény elkövetését.

A számítógép közreműködésével végrehajtott megtévesztő magatartásokat megkülönböztethetjük úgy is, hogy:

---

[126] BH. 1989/184.
[127] Dr. Pusztai id. mű ... M.J. 34.1987.11. 958.l.
[128] Dr. Pusztai id. mű ... M.J. 34.1987.11. 959.l.
[129] adja hírül Almási M.: Léghajó Manhattan felett. Bp. KJK. 1992. 102-103. lapon
[130] vö. A.N. Smith - W.J. Alexander - D.B. Medley... p. 402.

- a számítógép a csalás elkövetésének a *célja*: idetartozik a számítógép memóriájában vagy hajlékony-, kompaktlemezen tárolt adatok megváltoztatása haszonszerzés céljából.
- A számítógép *eszköz* is lehet a csalás végrehajtásához. E körbe vonható a szoftver- és a hardvermanipulálás. A hardvermanipulálás a komputernél ún. "egyszerűbb gépek" pl. a taxióra, mobil telefonok vagy a telefonkártya működésének átprogramozása tartozik. E utóbbi körből **hazánkban** a Btk. 1996. évi módosítását követően a közcélú mobil telefonok programjának hamisítását, és telefonkártyák végtelenítését stb. is büntetik.

A modi operandi egyes tipikus formái a szakirodalomban ironikus, sokszor groteszk elnevezéssel ismertek.[131]

- Data-diddling (adatok "lóvá tétele") nem más, mint adatváltoztatás az in-put fázisban.
- Trojan Horse (a "trójai faló"): a normál programmal egyidőben jogosulatlan műveleteket is végeztet a számítógéppel.
- Salami - technique programmal "lecsíphető" a számítógép üzemidejéből vagy a kezelt adatokból.
- Masquerad (álarcos bál) programmal az elkövető más személy nevét, kódját felhasználva veszi igénybe a számítógép szolgáltatásait.
- Piggyback (háton lovagol) programmal az elkövető az elektronikus adatfeldolgozó rendszerbe történő jogszerű belépést és/vagy használatot követően hajtja végre jogosulatlan cselekményét.
- Supperzapp ("csak veszély esetén használni") olyan program indítása, amikor a számítógépes rendszer leáll vagy hibásan működik, és kizárt a rendszert újraindítani a szokásos eljárásokkal. Viszont ezáltal lehetővé is válik jogosulatlan beavatkozás az elektronikus adatfeldolgozás- és átvitel folyamatába.

A számítógépes csalások kriminalizálását megelőzően ezeknek a jogsértéseknek a büntetőjogi értékelése nem kevés nehézségbe ütközött. A jogi minősítést övező tudományos diszkusszió és a joggyakorlat megosztott volt abban a

kérdésben, hogy a számítógéppel végrehajtott csalás beleillik-e a hagyományos csalás keretei közé-e vagy sem.

Az **osztrák** és a **német** joggyakorlatban annak a könyvelőnek a magatartását, aki számítógépét, illetve annak terminálját használva pénzt utal át saját, netán harmadik személy számlájára hatalommal való visszaélés bűncselekményének minősítette, azzal az indokolással, hogy az elkövető feladatkörét túllépve cselekszik.[132]

A számítógépes csalást akkor tekintik tradicionális csalásnak, ha az elkövető tevékenységének - akár in-put szakban, adatbevitelkor, akár out-put szakban, utalványozáskor - *emberi kontrollja* van. Ezzel ellentétes ítéletek születnek pl. Franciaországban, Hollandiában, Skóciában, Kanadában, míg Angliában, Walesben vitatják ezt.[133]

A *francia* Büntető Kollégium egyik határozatában megállapítja azt, hogy számítógépes csalás során az elkövető nem a gépet, hanem a gép mögött álló embert csapja mesterkedéseivel. [134]

A cselekmény minősítését nehezíti az, hogy a számítógép egyszerre a bűncselekmény elkövetésének a célja és eszköze. Az előbbi eset akkor jön szóba, amikor az adatok manipulálása történik a számítógép memóriájában, míg máskor a számítógép funkcióját használják fel az elkövetők a meg nem engedett művelethez. Az első esetben is a számítógép, mint eszköz jelenik meg, viszont ennek magatartásnak az elsődleges célja az adatok megváltoztatása. Más esetben az adatállomány manipulása akár szükségtelen lehet, viszont az adatállománnyal elvégzett művelet már tiltott.

A joggyakorlat ellentmondásossága utalt arra, hogy a jogalkalmazás észleli egy új típusú jogsértés létét és nem engedvén az elkövetőket az igazságszolgáltatás

---

[131] CE Recommendation ..... p. 18.(v.ö. 85.sz.) és v.ö. R.M. Stair p. 506.
[132] Revue ..... p. 1.
[133] CE Recommendation (89) 9. ..... p. 37. (v.ö. 85.sz.)52. (osztrák), p. 332. (német)
[134] R. Gassin id. mű .... 168.l.

"karmaiból" igyekezett a *nullum crimen sine lege* elvének megfelelően a már ismert tényállások közé szorítani, sokszor kissé mesterkélt - a törvényesség határait súroló - magyarázatokkal.

A számítógépes környezetben végrehajtott csalás minősítésének anomáliái sürgették a büntetőjogi fellépés feltételeinek egyöntetű megteremtését.

A nemzetközi judikatúrába történő betekintés során láthatjuk azt a trendet, hogy a számítógépes csalás önálló törvényi tényállásba foglalása a számítástechnikában fejlett országokban végbement. Magyarország a második hullámban csatlakozott e folyamathoz. Elöljáróban le kell szögezni, hogy az új törvényi tényállások kialakításának alapja az adott ország jogi tradíciói, így a Btk. Különös részének, ezen belül a vagyon elleni bűncselekmények rendszere, megfogalmazása.

A most következő, sajnos nem teljes körű jog-összehasonlításból ki fog derülni, hogy miként fejlődik - a modi operandi bővülésével párhuzamosan - a tényállásban értékelt elkövetési magatartások köre, hogyan kristályosodnak ki annak standard elemei.

Az első törvénytervezet - természetesen a számítógép szülőhazájában, akkoriban e téren hegemón szerepet játszó - **Egyesült Államokban** alkotják meg 1977-ben.

A "Szövetségi számítógépes rendszer védelméről" szóló törvény két évvel később születik meg. Ennek 240. §-nak a. pontja büntetni rendeli azt az elkövetőt, *"aki a törvényben felsorolt pénzügyi és kormányzati intézmények számítógépeit, számítógéprendszereit, -hálózatait, annak bármely egységét egészben vagy részben azért használja, használatát megkísérli vagy a annak használatát lehetővé teszi, hogy magának vagy másnak csalárd fondorlattal vagy más módon pénzt vagy szolgáltatást szerezzen."* [135]

Ezt követően a szövetségi államok törvényhozói látnak neki saját törvényeik kidolgozásához.

---

[135] Michael Gemignani: Law and the Computer. Boston 1981. p(s). 146-147.

A megszületett egyesült államokbeli jogszabályfolyamból érdemes kiragadni az arizonai tervezetet, amely először használja a számítógépes csalás elnevezést. E törvény a számítógép jogellenes használata, mint elkövetési magatartás mellett szankcionálta az adat- vagy programmódosítást is.[136] 1984-ben lát napvilágot az első speciális törvény az Egyesült Államokban "A jogellenes behatolással megvalósított számítógépes visszaélésekről illetve számítógépes csalásokról."

Földrajzilag, de még inkább a jogi hagyományokban hozzánk közelebb álló európai törvénykezések sorát Dánia nyitja meg 1985-ben.

A **dán** büntető törvénykönyv ekképp határozza meg a bűncselekményt: *"279/A. § Aki abból a célból, hogy magának vagy másnak jogtalan előnyt szerezzen az elektronikus adatfeldolgozáshoz használt adatot vagy programot jogosulatlanul megváltoztat, kiegészít vagy töröl vagy bármely más módon megkísérli az elektronikus adatfeldolgozás eredményét befolyásolni."* [137]

A dán Btk.-ban a számítógépes csalás önálló törvényi tényállás, amely a vagyon elleni bűncselekmények közt szerepel. Ebben a definícióban jelennek meg e bűncselekmény tipikussá váló objektív és szubjektív elemei.

A törvényi tényállás tárgyi oldalán értékelt elkövetési magatartások között:

- az adatok és/vagy programok megváltoztatása,
- azok kiegészítése,
- törlése vagy
- az elektronikus adatfeldolgozás egyéb módon történő befolyásolása.

A cselekmény célzatos, az elkövető törvényi tényállásban értékelt célja a jogosulatlan vagyoni haszonszerzés.

---

[136] Dr. Pusztai id. mű: KKT. XXVI. sz. 111-113.l.

[137] Albin Eser - Jonatan Thormondson: Old Ways and Needs in Criminal Legislation - Documentation of a German - Icelandic Colloquium on the Development of Penal Law in General and Economic Crime in Particular. Freiburg, 1989. p. 252.

A bűncselekmény megfogalmazása a hagyományos csalás struktúráját (jogtalan haszonszerzés végett történő megtévesztés) követi.

A **német** Btk.-ban az 1987-es módosítás folytán válik büntetendővé ez a cselekmény:

„263/A. § (1) Aki abból a célból, hogy magának vagy egy harmadik személynek jogellenes vagyoni előnyt biztosítson, más vagyonát azáltal károsítja, hogy az adatfeldolgozási folyamat eredményét a program helytelen kialakításával, helytelen vagy hiányos adatok felhasználásával, adatok jogosulatlan felhasználásával vagy a feldolgozás folyamatára való egyéb jogosulatlan ráhatással befolyásolja, öt évig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő." [138]

Ez a meghatározás a tradicionális csalás alapesetével együtt szerepel a Btk.-ban. Minősített esetük közös.

A német törvényjavaslat vitája során - ahogy azt a jóemlékű **Pusztai László** felidézi - a számítógépes csalást a tradicionális csalás minősített eseteként gondolták. Ám az elméleti állásfoglalások hatására önálló tényállássá válik.[139] Kissé bizarrnak hatna az az elképzelés, hogy egy számítógép "megtévesztése" súlyosabban minősülne, mint valamely természetes személyé.

A bűncselekmény tárgyi oldala nem azonos a dán tényállás objektív elemeivel. Az "elkövetési tárgy" csupán a helytelen vagy hiányos adatokra szűkül, ellenben eredményként értékelendő a más vagyonában bekövetkezett kár. A német **Otto Harro** szerint ez a tényállás alkalmas a bankkártyával visszaélés minősítésére is.[140]

---

[138] Dr. Pusztai id. mű: .... KKT. XXVI.sz. 114-115.l.

[139] Dr. Pusztai id. mű: .... KKT. XXVI.sz. 111-112.l.

[140] Dr. Harro Otto: Übungen im Strafrecht. Berlin * New York, 1995. s(n). 125-126., és Revue ... p. 342.

Ugyanebben az évben születik e bűncselekmény **japán** jogi szabályozása. Ennek megfogalmazása szintén meglehetősen technicizált. Az ottani Btk. kimondja: *"246-2. § Aki hamis elektromágneses rekorddal jelölt vagyoni előny, veszteség megjelenítését, vagy más vagyoni jogok módosítását eredményező hamis adatok vagy utasítások bevitelével vagy egyéb módon beavatkozik más személy számítógépesített üzletmenetébe, és ezzel jogtalan előnyt szerez vagy kárt okoz tíz évig terjedő szabadságvesztéssel büntetendő."* [141]

A japán Btk.-ban ez a cselekmény - hasonlóan a német megoldáshoz - a tradicionális csalás második alapesete. A tényállás tárgyi oldalán az elkövetési magatartásokat kevésbé részletezően fogalmazzák meg. A bűncselekmény eredménye vagylagosan jogtalan előny, illetőleg kár.

A következő évben módosított **osztrák** Btk. az alábbi meghatározással egészül ki:

"148/a. § (1) Aki szándékosan magának vagy másnak jogtalan előnyt szerezve harmadik személynek kárt okoz program kialakításával, adatok bevitelével, megváltoztatásával vagy törlésével, illetve az elektronikus adatfeldolgozás eredményének más módon történő befolyásolásával 6 hónapig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő.

(2) A büntetés 3 évig terjedő szabadságvesztés, ha a kár 25.000.- schillinget, továbbá 10 évig terjedő szabadságvesztés, ha a kár 500.000.- schillinget meghaladja." [142]

Ausztriában már 1985-ben elkészül a számítógépes bűncselekmények tervezete. Ekkor a deliktum a "számítógépes csalás" elnevezéssel szerepel, a tényállás neve "csalárd visszaélés az adatfeldolgozással". A tényállás rendszerbeli

---

[141] Revue ... p. 444.

[142] Strafgesetzbuch 10., durchgesehene Auflage. Wien (Manz * Taschenausgaben) 1990. s(n). 141-142.

helye megegyezik más országok szabályozásával. A csalárd visszaélés az adatfeldolgozással a tradicionális csalás tényállását követi a Btk.-ban.

Jogértelmezési vitát vált ki nyugati szomszédunkban az, hogy a törvényhozó mellőzi a jogellenes jelzőt az elkövetési magatartások meghatározásánál, továbbá nem utal az adatok hiányos és helytelen voltára.[143]

A **görög** 1805/88. számú törvény vezeti be a számítógépes csalás fogalmát. A meghatározás kialakítása rendkívül hasonló a német szabályozáshoz, amennyiben görögh onban is az minősül számítógépes csalásnak, ha az elkövető magának vagy másnak úgy szerez vagyoni előnyt, hogy a számítógépbe helytelen vagy hiányos adatot táplál be, a számítógépet helytelenül programozza vagy más módon avatkozik be jogosulatlanul az elektronikus adatfeldolgozás folyamatába, amely az adatfeldolgozás eredményét befolyásolja. (Görög Btk. 386/A. §)[144] Ezen tényállás szerint felel az elkövető, ha bankkártyájával visszaél.

A **svéd** Btk. 1990-től bünteti a számítógéppel megvalósított csalást. Ennek megfelelően: *"csalást követ el az is, aki helytelen vagy hiányos adatok felhasználásával, a program megváltoztatásával, készítésével vagy bármely más módon az automatikus adatfeldolgozás, továbbá más egyszerű feldolgozás jogtalan befolyásolásával magának előnyt szerez vagy másnak kárt okoz." (9. fejezet 1.§)*[145]

E tényállás a tradicionális csalás alapesetét követi a kódexben, minősített esetük közös. Ennyiben hasonló a német szabályozáshoz.

A bűncselekmény jogi tárgya bővül, mivel a büntetőjogi védelmet kiterjesztették az egyéb *egyszerű adatfeldolgozási folyamatokra* is. Azzal az indokolással, hogy a pénzért árusító- vagy szolgáltató automaták manipulálásának minősítésekor felmerülő vitáknak elejét vegyék. Amíg pl. Japánban vitatott a

---

[143] Revue ... p. 151-154.
[144] Revue ... p. 367-368.
[145] Revue ... p. 581.

manipulált telefonkártyákkal való visszaélés[146], Svédországban ez megoldottnak tűnik. A svéd szabályozás további sajátossága, hogy a tárgyi oldalhoz tartozó jogtalan előny vagylagos az okozott kárral. Ez viszont a japán Btk. megoldásával rokon.

A **finn** törvénymódosítás a 100. éves finn Btk. évfordulójának tiszteletére 1991-ben születik. A számítógépes csalás fogalma az alábbi:
"Módosító novella 36. §: Csalást követ el az is, aki hamis adat bevitelével vagy az elektronikus adatfeldolgozás folyamatára történő egyéb beavatkozással meghamisítja a műveletek eredményét, és ezzel másnak kárt okoz két évig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő.
A kísérlet is büntetendő." [147]

A szabályozás módszere hasonló a német valamint a svéd megoldáshoz, vagyis a számítógépes csalás, és a tradicionális csalás képezi az alapesetet, ezt követi a közös minősített eset.

Az 1991-es **svájci** Btk.-ban a "csalárd visszaélés az adatfeldolgozási folyamattal" törvényi tényállása a következő:
"147. § (1) Aki szándékosan magának vagy másnak jogtalan előnyt szerez helytelen, hiányos, vagy az adatok jogtalan használatával, vagy egyéb módon az elektronikus adatfeldolgozás- és átviteli folyamatot befolyásolja, a megszerzett vagyoni előnyt elrejti, és ezzel vagyoni kárt okoz egy harmadik személynek öt évig terjedő fegyház- vagy börtönbüntetéssel büntetendő.
(2) A büntetés tíz évig terjedő fegyház- vagy börtön, ha a bűncselekményt üzletszerűen követik el." [148]

---

[146] Revue ... p. 445.
[147] Centenary of the Finnish Penal Code ... id. kiadvány (v.ö. 97.sz.) p. 15. - saját fordítás.
[148] www.gesetze.ch/sr/311.0/311.0_012.htm - saját fordítás.

A számítógépes csalást szintén a hagyományos csalás mellé helyezik el a svájci Btk.-ban. A deliktum tárgyi oldalán az elkövetési magatartások sora bővül: a "megszerzett vagyoni előny elrejtése". Itt arról az esetről van szó, amikor az elkövető nem realizálja a jogtalan vagyoni előnyt (nem utalja saját vagy más számlájára, nem veszi fel pénztárban stb.), hanem a számítógép memóriájában, csak az általa ismert, kódokkal védett file-ba viszi, ott tárolja vagy az adatállományt kódolja.

A **spanyol** törvény 1992-ben készül el és a tradicionális csaláshoz lakonikusan annyit fűz: *"csalás az is, aki haszonszerzési céllal manipulálja a számítógépet és ezzel a beavatkozással az adatfeldolgozás- vagy az átvitel eredményét befolyásolja." /248-2. §/* [149]

Az **olasz** törvénymódosítást 1993. december 30-án hirdetik ki. Ennek idevonatkozó rendelkezése szerint:
"640. (kiegészítő) §: Aki bármely módon megváltoztatja egy informatikai vagy teleinformatikai rendszer működését, vagy jogtalanul beavatkozik az informatikai, teleinformatikai rendszerbe, a rendszerben levő adatokba, információkba vagy programokba és ezzel magának vagy másoknak jogtalan hasznot szerez, avagy másnak kárt okoz 3 évig terjedő szabadságvesztéssel vagy százezer lírától kétmillió líráig terjedő pénzbüntetéssel büntethető." [150]

A büntetés akár öt évig tartó szabadságvesztésig, illetőleg a pénzbüntetés összege hatszázezer lírától hárommillió líráig is terjedhet, ha a bűncselekményt a rendszeroperátor követi el (delicta propria).

---

[149] Preliminary/Draft Versions.... for the Computer Crime Conferences in Würzburg. Würzburg 1992. p.(s) 302-304.

[150] Leggi, decreti e ordinanze presidenzali ... id. közlöny (v.ö. 98. sz.) 7.1. - saját fordítás.

A számítógépes csalás szabályozásának ismertetett példáiból levonható **tanulságok** a magyar jogalkotás számára:

1. A számítógépes csalás rendszerbeli helyét tekintve általában a hagyományos csalás tényállása mellé rendelt. Meg kell jegyezni, hogy pl. a német, az osztrák és svéd büntető törvénykönyvekben a gazdasági bűncselekményeket nem szabályozzák külön fejezetben.

Viszont egyértelműen látható, hogy a *hagyományos csalást* tekintik a szabályozás alapjának, példájának.

2. A számítógépes csalás büntetni rendeltsége vagy a hagyományos csalás kiterjesztő értelmezése által (pl. Svédországban, Spanyolországban) vagy önálló tényállásban (ahogy pl. Németországban, Ausztriában) valósul meg.

3. Elkövetési magatartások: helytelen vagy hiányos adat betáplálásával, adatok törlésével, változtatásával, elrejtésével, program módosításával vagy - nyitottá téve a tényállást - az elektronikus adatfeldolgozás egyéb módon való befolyásolásával követhető el.

A svájci szabályozás szövegében az elektronikus adatátviteli folyamat befolyásolása is büntetendő.

4. A számítógépes csalás, mint eredménytényállás került kialakításra. Eredményként a számítógép manipulálásával okozott kár szerepel.

A nyolcvanas évek végén **Magyarországon** is követnek el számítógéppel csalásként értékelhető bűncselekményeket. A terhelt számítógépes programozóként dolgozik a vállalatnál. Munkavégzésének helye az a gépterem, ahol a vállalat számára érkező befizetéseket könyvelik számítógéppel. A vádlott a munkáltató kezelésében lévő lakásban lakik. Fél év alatt megközelítőleg 2.900.- ft. lakbérhátralékot halmoz fel. Ezt a tartozását úgy egyenlíti ki, hogy a gépterem ellenőrzésének hiányosságait kihasználva saját kódszámán 3.000.- ft. befizetését billentyűzi be a gépbe. Tevékenységével a számítógépben tárolt adatokat meghamisítja. Másnap az ellenőrzés során derül fény arra, hogy az adatbevitel mögött nem állt tényleges befizetés.

Az első fokú bíróság csalás kísérletében és magánokirat-hamisításban mondja ki a vádlott bűnösségét. Az akkor hatályos büntető-eljárási törvény ismeri a törvényességi óvás intézményét, amely akkori formájában 1992-ig funkcionál. Törvényességi óvást jogerős ítéletek ellen, akár a terhelt javára, akár - igaz, korlátozottan - a terhére lehetett benyújtani. Jelen esetben a terhelt javára nyújtanak be törvényességi óvást a csalást minősítő és a magánokirat-hamisítás vétségében megállapító rendelkezés ellen.

A csalás minősítését illetően a Legfelsőbb Bíróság arra a megállapításra jut, hogy a csalás bűncselekménye eljutott a befejezettség stádiumáig. Indokolásában a bíróság kifejti, hogy a terhelt saját kódszámán fiktív befizetést eszközölt. Megtévesztő magatartásával azt a hamis látszatot kelti, hogy tartozása ki van egyenlítve. Ebben a helyzetben a vállalat vagyonában már beáll az értékcsökkenés. "Ezáltal tehát a csalás *valamennyi törvényi tényállási eleme* megvalósult, és a bűncselekmény befejezetté vált."

Ugyanakkor a Legfelsőbb Bíróság megállapítja azt is, hogy az első fokú bíróság törvényt sért, amikor a terhelt bűnösségét a magánokirat-hamisítás vétségében is kimondja. A magánokirat-hamisítás bűncselekménye jog vagy kötelezettség létezésének, megváltoztatásának vagy megszűnésének bizonyítására hamis, hamisított vagy valótlan tartalmú magánokirat használatában áll. (Btk. 276. §)

A bűncselekmény hamis adatok számítógépbe történő bevitelével valósul meg, tehát a terhelt nem használt semmilyen okiratot sem. Ezáltal hiányzik a magánokirat-hamisítás egyik legfontosabb tényállási eleme.

A Legfelsőbb Bíróság magánokirat-hamisítás vétsége miatt emelt vád alól a terheltet bűncselekmény hiányában felmentette.[151] A LB. ítéletének ezen része kétségkívül nem vitatható.

Azonban a csalás bűncselekményének megállapítása - véleményem szerint - igencsak aggályos. A magyar Btk. szerint: *"aki jogtalan haszonszerzés végett mást*

---

[151] BH. 1989/184.sz.

tévedésbe ejt vagy tévedésben tart és ezzel kárt okoz, csalást követ el." (Btk. 318. § (1) bekezdés)

A csalás valamely *természetes személy* tévedésbe ejtése vagy tévedésben tartása folytán jön létre. Az elkövetési magatartással okozati összefüggésben kell a sértett oldalán vagyoni kárnak, mint eredménynek keletkeznie. A bűncselekmény passzív alanya olyan természetes személy is lehet, aki a sértett vagyona vonatkozásában jogszabály vagy polgárjogi aktus (pl. megbízás) alapján ténylegesen rendelkezik.

A csalás két mozzanatú bűncselekmény. Az első fázisban a passzív alany tévedésbe ejtése vagy tévedésben tartása történik. Ennek alkalmasnak kell lennie arra, hogy a sértettben a valóságtól eltérő képzet keletkezzen vagy a már létező hamis képzetet fenntartsa, megerősítse. De a megtévesztésnek (fraus criminalis) alkalmasnak kell lennie arra is, hogy a sértettet vagyoni hatású cselekményre is indítsa. Ezt nevezi a német **Robert von Hippel** a XX. század első évtizedeiben "burkolt tényállási elemnek".[152] Ez valósul meg a csalás második fázisában. Vagyis a megtévesztett személy - e téves tudatán alapuló - akaratával adekvát vagyoni rendelkezést tesz. A sértett - tehát - tévedése következtében szenved vagyoni kárt. Viktimológiai közelítéssel azt is mondhatjuk, hogy a sértett vagy vagyoni viszonyai körében a rendelkezésre jogosult más személy döntésétől függ a bekövetkezett kár nagysága. Ebben az esetben viszont hamis adatok bevitelét követően a számítógép a programjának megfelelően kiegyenlítettnek számítja az elkövető lakbérhátralékát, azt kell mondanunk, hogy a gép automatikusan "tett" vagyoni hatályú rendelkezést. Az ügyintéző csupán a vállalat vagyonában bekövetkezett tényleges értékcsökkenés *után* észlelte, észlelhette a kár beálltát. Tehát a csalás tényállásában szereplő *természetes személy*, a passzív alany, mint tényállási elem itt (is) *hiányzik*. Ebből következően az nem mondható ki, hogy "a csalás *valamennyi törvényi tényállási eleme* megvalósult, és a bűncselekmény befejezetté vált."

---

[152] Dr. Angyal Pál: A csalás. (A magyar büntetőjog kézikönyve 16. kötet.) Budapest. 1939. 67-68.l.

Felmerülhet a kérdés, hogy a számítógép üzemeltetőjének, kezelőjének megtévesztése fennforog-e vagy sem?

A számítógép üzemeltetőjének, kezelőjének a hamis adat bevitelről a bevitel időpontjában nincs tudomása. Ugyanígy a számítógép programjának megfelelő "döntéséről" sem.

A csalás bűncselekményének második fázisa nem valósul meg, ha "tűrésnek" is tekintenénk, akkor sem értékelhető - akár utólagos, akár passzív - vagyoni rendelkezésnek. A számítógép kezelője vagy üzemeltetője csupán utólag konstatálhatja vagyoni veszteségét.

Más lenne a helyzet, ha a hamis adat bevitel, és a vagyoni rendelkezés közötti időben megismeri a megtévesztésre szánt hamis adatokat, és ezek tudatában dönt úgy, hogy nem avatkozik be az elektronikus adatfeldolgozás folyamatába. Ez esetben valóban megállapítható lenne a csalás bűncselekménye. Ezek hiányában viszont magatartása nem értékelhető a Btk. 318. §-ba ütköző csalás bűncselekményeként.

Mivel a terhelt tevékenysége a törvényben meghatározott bűncselekmények egyikének sem felelt meg, így ellene a büntető eljárást bűncselekmény hiányában meg kellett volna szüntetni.

A hazai szakirodalomban **Pusztai László** tesz kísérletet a számítógépes csalás tényállásának megfogalmazására. Ez tükrözi a nyugat-európai jogfejlődés ismeretét és e bűncselekmény sajátosságait. Elképzelésével egyetértek. Szerinte a számítógépes csalás a tradicionális csalás egyik esete lett volna: "csalást követ el az is, aki jogtalan haszonszerzés végett azzal okoz kárt, hogy az adatfeldolgozási folyamat eredményét a program helytelen kialakításával, helytelen vagy hibás adatok felhasználásával vagy a feldolgozás folyamatára való egyéb jogtalan ráhatással befolyásolja."[153]

---

[153] Dr. Pusztai .... id. mű KKT. XXVI.sz. 145.l.

A büntető törvénykönyv gazdasági bűncselekményekről szóló fejezetének átdolgozásakor, a kormány által beterjesztett Javaslatban a számítógépes csalást és a bankkártyával visszaélést is ebbe a körbe sorolják. A Javaslat szerint a számítógépes csalás alapesetét az követi el: "aki jogtalan haszonszerzés végett valamely számítógépes adatfeldolgozás eredményét a program megváltoztatásával, törléssel, téves vagy hiányos adatok betáplálásával, illetve egyéb, meg nem engedett műveletek végzésével jogellenesen befolyásolja, és ezzel kárt okoz, bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő." [154]

A számítógépes csalás első megfogalmazásakor tehát a tradicionális csaláshoz hasonlóan, annak célzatára, vagyis a jogtalan haszonszerzés céljára helyezik a hangsúlyt, míg az elfogadott törvény az elektronikus adatfeldolgozás befolyásolását, mint elkövetési magatartást nyilvánítja büntetendővé.

Az európai jogfejlődés felvázolásakor látható, hogy azokban az országokban, ahol ezt a cselekményt kriminalizálják, ott azt - általában - a hagyományos csalás tényállásához kötik.

Úgy is tekinthetjük, hogy a megtévesztéssel történő jogtalan vagyoni haszonszerzés *repertoárja* bővül ki napjaink legmodernebb eszközével, a számítógéppel.

E tény értékelése jogbizonytalanságot idézett elő, amelyet - zömmel - új tényállás beiktatásával küszöbölnek ki. Éppen ebből a megfontolásból ezt a bűncselekményt - ma még - a vagyon elleni deliktumok közé sorolnám.

A bűncselekmény megnevezése nem fedi a tényállásban meghatározott cselekmény jellegét. A csalás elnevezés, immár évszázadok óta olyan bűncselekményt takar, amely - **Angyal Pál** szavaival élve - "lényegileg abban áll, hogy valaki a tettes által vagyoni haszonszerzés céljából előidézett vagy egyébként már létező, de a tettes által kihasznált tévedés hatása alatt saját vagy más vagyoni kárára oly rendelkezést tesz, melynek jelentőségét, és illetőleg kártokozó következményét tévedésénél fogva nem ismerte fel." [155]

---

[154] Büntetőjogi és Kegyelmi Ügyosztály 35.135/1992. IM. III. 16. §
[155] Dr. Angyal Pál: A csalás ... id. mű 35.l.

A tényállás elfogadott szövegében azonban nemcsak a csalás sajátosságai szerepelnek, hanem egy a hagyományos rongáláshoz hasonlítható károkozó cselekmény elemei is.

Az 1994:XVII. törvény 16. §-a alkotja meg a számítógépes csalás tényállásának (1) és (2) bekezdését, majd ezt az 1996. évi LII. törvény 19. §-a egészíti ki a (3) bekezdéssel, és végül az 1999:CXX. törvény módosítása által az alábbiak szerint hatályos:

300/C. § (1) Aki jogtalan haszonszerzés végett vagy kárt okozva valamely számítógépes adatfeldolgozás eredményét a program megváltoztatásával, törléssel, téves vagy hiányos adatok betáplálásával, illetve egyéb, meg nem engedett műveletek végzésével befolyásolja,

bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés

a./ öt évig terjedő szabadságvesztés, ha a számítógépes csalás jelentős kárt okoz,

b./ két évtől nyolc évig terjedő szabadságvesztés, ha a számítógépes csalás különösen nagy kárt okoz.

c./ öt évtől tíz terjedő szabadságvesztés, ha a számítógépes csalás különösen jelentős kárt okoz.

(3) Számítógépes csalást követ el az is, aki az (1)-(2) bekezdésben írt cselekményt közcélú mobil rádiótelefon szolgáltatás igénybevételére szolgáló elektronikus kártya felhasználásával, vagy közcélú mobil telefont vezérlő mikroszámítógép programjának megváltoztatásával követi el."

A számítógépes csalás jogi tárgya vagyoni viszonyok, amelyek adatokban ölt formát, és amelyek tartalmukban vagyoni követelések vagy jogosultságok, - esetlegesen olyan kötelmi jogviszonyt is jelölhetnek, amelyek pénzmozgást tükröznek. Ez utóbbi nemcsak létező, de jövőben keletkező jogviszony is lehet. Elkövetési adat a számítógépes adat, amely nem más, mint elektronikus impulzus.

A bűncselekmény tárgyi oldalán szereplő elkövetési magatartás elemzését - új jelenség lévén - részleteznem kell. Az elektronikus adatfeldolgozási tevékenység

befolyásolásának körébe tartozik a program megváltoztatása, adatok törlése, téves vagy hiányos adatok betáplálása, továbbá bármilyen más olyan tevékenység (pl. az inkriminált adatok elrejtése, "titkosítása") - itt válik nyitottá a tényállás - amely alkalmas arra, hogy az elektronikus adatfeldolgozás eredményét befolyásolja.

- A program megváltoztatása: az elektronikus adatfeldolgozás rendeltetésének, céljának megfelelő program részben vagy egészben történő átírása vagy annak részleges törlése. Ezek kombinációja. Továbbá minden olyan utasítás felvitele, amelynek révén meg nem engedett műveletek végezhetők.

- Az adatok törlése: az adatállományt alkotó adatok teljes körű vagy részleges eltávolítása, amely megvalósulhat törlés- (delete-) funkcióval vagy felülírással (typeover - funkcióval), mágnesszalagok elektromágneses úton való törlésével stb. A részleges deleálás esetén nem szükséges, hogy az adatok felismerhetetlenekké váljanak.

- Téves vagy hiányos adatok betáplálása. Téves az adat, amely nem tükrözi a valóságot. Hiányos az adat, amely csupán a valóság egy részét tükrözi.

Az adatok betáplálása történhet azok bebillentyűzésével a számítógép klaviatúráján, vagy olyan adathordozóról (lemez, mágnesszalag, lyukkártya, lyukszalag stb.) történő adatbehívással, amelyre korábban rögzítették a téves vagy a hiányos adatokat.

A bűncselekmény alanyi oldalát tekintve a számítógépes csalás elkövetője bárki lehet. Kriminológiai tapasztalat az, hogy a potenciális elkövetői kör zöme azokból kerül ki, akik a pénzmozgásokat rögzítő elektronikus adatfeldolgozás folyamatában - közvetlenül - részt vesznek (pl. operátorok, programozók) vagy ott könnyedén hozzáférhetnek a számítógépekhez.

Viszont a számítógépes hálózaton keresztül - ezáltal közvetett módon - történő hozzáférés technikai lehetőségével bárki válhat a bűncselekmény elkövetőjévé.

A bűncselekmény alanyi elemei közül ki kell emelnem a jogtalan haszonszerzésre irányuló célzatot (animus lucri), és ezzel vagylagosan a károkozásra irányuló szándékot (animus nocendi). A célzat megléte az iránymutató

joggyakorlat szerint az egyenes szándékra korlátozza az elkövető bűnösségét. Ez a célzat akkor állapítható meg, ha az elkövető bűncselekményével vagyonát kívánja növelni, akár vagyoni aktívumának gyarapításával, akár passzívumának csökkentésével. A károkozás fogalmába beleértendő - az ET. (89) 9. sz. Ajánlásának alternatív javaslata alapján - a passzív alany vagyonától való megfosztás is.[156]

A bűncselekmény passzív alanya nemcsak természetes, hanem jogi személy is lehet. E bűncselekmény sértette az, akinek az érdekében folyik az elektronikus adatfeldolgozás. Ez utóbbi megállapítás akkor releváns, ha a passzív alany ezt a tevékenységet más cégnél végezteti el.

A számítógépes csalás eredménye: a kár, ami a Btk. 137.§ 5.pontja szerint (legis interpretati): "bűncselekménnyel a vagyonban okozott értékcsökkenés". Ez a definíció nem fedi a kár civiljogi fogalmát.

Csak a károsult (akár természetes, akár jogi személy) vagyonában beállott tényleges kár (*damnum emergens*) jöhet figyelembe.

Jelenleg a jelentős kár érték a 2 millió és az 50 millió közötti, a különösen nagy érték az 50 millió és az 500 millió ft. közötti, a különösen jelentős érték az 500 millió ft. feletti kárérték.

Az elmaradt vagyoni előny (*lucrum cessans*) a büntetőjogi kárértékként nem értékelhető. Ezt, valamint a helyreállításhoz szükséges költséget, kárpótlást a büntető eljárásban polgárjogi igényként vagy civiljogi eljárásban érvényesítheti a sértett. Mivel a magyar jogrendszerben két jogág eltérő kár fogalmat határoz meg és ez zavaró lehet a büntető eljárásban. Egyetértek **Siegler Eszterrel** aki szerint a büntetőjogi kár fogalmát a civiljogi kár fogalmához kellene igazítani. [157]

A bűncselekmény (3) bekezdése az elektronikus adatfeldolgozás egy speciális formájának jogosulatlan befolyásolását bünteti.

---

[156] CE Recommendation (89) 9.: Appendix I. p(s). 105-106.

[157] . Dr. Siegler Eszter: A számítógéppel kapcsolatos és a számítógépes bűncselekmények. MJ. 44. 1997. 12.sz. 741.l.

Osztjuk a kódexmódosítás kapcsán **Tóth Mihály** által írott véleményét, e szerint "nem látszik szerencsésnek a módosítás... mert a (3) bekezdésben szereplő szerkezetek felsorolása révén a jogalkotó akaratlanul is a taxáció itt semmiképpen sem kívánatos mezejére tévedt."[158]

A hamisított telefonkártyák felhasználása adatbeviteli (in-put) adatmanipulálásként értékelhető és ugyanígy a mobiltelefon chipjén található adatok jogosulatlan megváltoztatása is olyan adatmanipulálás, amely alkalmas az elektronikus adatfeldolgozás eredményét befolyásolására, így nevesítésük talán el is maradhatott volna, hiszen nem szükséges egy-egy számítógép vezérelte rendszert kiemelni. Ma már szinte minden háztartási vagy más elektronikus gépben, autóban, órában számítógép fellelhető miniatűr szerkezet, amely funkciójában megegyezik számítógép rendeltetésével. Arról nem is beszélve, hogy maga a telefonkártya eleget tesz a számítógép funkciójának: adatot tárol, műveletet végez stb. Ugyanakkor a joggyakorlatban komoly kérdést vet fel az, hogy a taxióra számítógépnek minősül-e vagy sem. **Siegler Eszter** idézi a Fogyasztóvédelmi Főfelügyelőség állásfoglalását, amely szerint "a mai modern taxiórák megfelelnek a számítógép ismérveinek ..... számításokat végezve tájékoztatja az utast az aktuális viteldíjról, a szolgáltatás igénybevételének végén a fizetendő összegről ..... számlát is képes kinyomtatni. Ezenkívül a taxióra alapján ellenőrzi az adóhivatal is a személyszállító kisiparosok tevékenységét, és teheti azért, mert a készülék munkanap végén az adatokat memória egységében letárolja." [159]

Ezzel szemben a Pesti Központi Kerületi Bíróság egyik ítéletében megállapítja, hogy "a Büntető Törvénykönyvhöz írott Kommentárban foglalt iránymutatás szerint a számítógép olyan elektronikus adatfeldolgozó eszköz, amely önállóan képes bonyolult számítási adatbeviteli és adatmegjelenítési feladatokat nagy gyorsasággal elvégezni. A taxióra is méri és kimutatja a különböző tarifa kulcsok szerinti utakat, és viteldíjakat, valamint memóriával is rendelkezik, azonban

---

[158] Dr. Tóth Mihály: Gazdasági bűncselekmények az alakuló joggyakorlatban. Budapest 1997. 210.l.

[159] Dr. Siegler Eszter: A számítógéppel kapcsolatos .... id. mű 741.l.

ezek a képességei még nem emelik a bíróság álláspontja szerint a számítógép kategóriájába, annál egyszerűbb szerkezet." [160]

Megítélésem szerint annak eldöntéséhez, hogy milyen készülékek tekinthetők számítógépnek, és melyek nem - számítástechnikai szakemberek véleményét kikérve - a Legfelsőbb Bíróság jogértelmezése adhat választ.

Összefoglalva az alábbi jogalkotási valamint jogalkalmazási *aggályok* vethetők fel a Btk. 300/C. §-szal kapcsolatban:

1. A jogalkotást érintően:

1.a. Megkérdőjelezhető a bűncselekmény Különös részi rendszerbeli helye. A nemzetközi tapasztalatok azt mutatják, hogy az európai országokban inkább a tradicionális csalással együtt szerepel. Igaz, hogy nem minden országban különül el a vagyon elleni és a gazdasági bűncselekményeket felölelő fejezetek.

1.b. A számítógépes csalás kriminalizálását megelőzően az érdeklődő szakma ismervén Pusztai László definícióját, majd a beterjesztett törvényjavaslatot egy a hagyományos csalással konkuráló szabályozást "várt". Az elfogadott törvény az elektronikus adatfeldolgozás befolyásolását bünteti, akár azt haszonszerzési célzattal, akár kárt okozva követik el.

1.c. A tényállás megnevezése "számítógépes csalás", ám szövegében nemcsak a csalás sajátosságai, hanem a hagyományos rongáláshoz hasonló károkozó magatartás elemei is szerepelnek. Ezáltal ellentmondás mutatkozik a cím és a tartalom között. Ez feloldható akár úgy, hogy a számítógépes csalás mellett majdan az adatfeldolgozás elleni intellektuális támadás szabályozására is sor kerül. Ez utóbbi bűncselekmény-kategória majdan "az elektronikus adatfeldolgozás- és adatátvitel akadályoztatása" kell, hogy legyen.

A tényállás (3) bekezdésének kialakítása egyetlen szempontból tanulságos. A hamis telefonkártyák használata, analóg telefonok többszörözése stb. még inkább

---

[160] PKKB. 16.B.IX. 4384/1996/7.sz.

feltárja a számítógépes csalás igazi "arcát", azaz nem más, mint haszonszerzés végett végrehajtott adatbeviteli manipuláció.

1.d. A tényállás (3) bekezdése az elektronikus adatfeldolgozás egy speciális formájának jogosulatlan befolyásolását bünteti. Semmi sem indokolja valamely elektronikus adatfeldolgozási rendszer nevesítését, kiemelését e tényállásban. Gondoljunk arra, hogy a taxiórák manipulálása szintén tipikusnak nevezhető.

2. *Értelmezési nehézségek* a jogalkalmazás terén:

2.a. Azzal, hogy a tényállás alapesete immateriális, lévén "az elektronikus adatfeldolgozás befolyásolását" rendelte büntetni, viszont a minősített esetek eredménytényállások, büntetendőségük a cselekménnyel okozott kárértékéhez (jelentős, illetve különösen nagy kár bekövetkeztéhez) igazodik. Ez a szabályozási mód rendkívül megnehezíti a jogalkalmazás számára a minősített eset *kísérletének* megállapítását.

2.b. A hamis, hamisított telefonkártyával összefüggésben még további jogalkalmazási problémák merülnek fel: a kártya hamisítása a 300/C. (1) bekezdésébe ütköző cselekmény, a felhasználása ugyanezen törvényhely (3) bekezdésébe ütközik. Véleményem az, hogy a hamis, hamisított telefonkártya használata (mivel a bűncselekmény kísérletéhez legalább egy billentyű leütése) általában tettenéréssel bizonyítható. Vagy aránytalan nyomozati cselekményekkel érhető el eredmény pl. videokamera alkalmazása.

A kísérletként nemcsak legalább egy billentyű benyomása értékelendő, hanem az az eset is, amikor a vádlott hamisított kártyájával sikertelen hívást kezdeményez.[161]

A számítógépes csalás tényállása felülvizsgálata kapcsán *de lege ferenda* megfontolandó:

- a Btk. 300/C. § (3) bekezdésének hatályon kívül helyezése,

---

[161] BKKB. 2.B.XI. 2671/1997/6.sz.

- a bűncselekmény valódi jellegének megjelenítése elérhető az 1994-es javaslattal vagy
- a Pusztai László által adott meghatározással, (mindkettő jól tükrözi az európai jogalkotás trendjét) vagy
- a hagyományos csalás (Btk. 326. §) tényállását egy kiterjesztő értelmezéssel alkalmassá tehető a számítógépes csalás büntetendővé nyilvánítása. Ahogy teszik a skandináv országok. Ez utóbbi előnye a jogalkalmazás során felbukkanó ama bizonytalanság megszűnése, amely a számítógépes csalás és a hagyományos csalás elhatárolásánál felmerül, ha a számítógép játszik szerepet a bűncselekmény elkövetése során.

Felvethető az ún. "egyszerű számítógépes rendszerek" (telefonkártyák, taxiórák stb.) jogtalan haszonszerzés végett végrehajtott manipulációjának a kriminalizálása is. Megítélésem szerint ez túlszabályozást jelentene és nem kevés bizonytalanságot, ellentmondó szakértői véleményeket arról, hogy mi tekinthető "egyszerű számítógépes rendszernek", hiszen törvényi taxatív felsorolás minden bizonnyal nem adható.

A számítógépes csalás kriminalizálásával a hagyományos csalás és más vagyoni bűncselekményekkel a törvényhozó versengést teremtett. A konkuráló tényállások között tehető dogmatikailag megnyugtatóan tisztázott különbségtétel még nem történt meg.

Kevés gyakorlati eset és nem több elméleti munka még nem elegendő - általános következtetések levonására.

A **német Btk. Kommentárjában** rögzítik, hogy a számítógépes csalás és a csalás elhatárolása bizonytalan. Kiindulópontja a kár, mint a tényállás tárgyi elemének fogalma. Ebből következik, hogy a csalás önkárosító bűncselekmény, a számítógépes csalásnál ez a közrehatás nem jellemző, ám bank- és más kártyákkal történő visszaélés esetében idegen személy károsító tevékenységével állunk szemben.

Másik jellemző vonás az, hogy a befolyásolt adatfeldolgozás közvetlenül idéz elő a kárt a sértettnél. Ha a kár közvetett úton következik be pl. számítógéppel manipulált nyomtatvány (pl. gáz-vagy villanyszámla) miatt fizet a sértett akkor az a hagyományos csalás tényállását meríti ki. [162]

Hazánkban **Tóth Mihály** azon az álláspontón van, hogy a számítógépes csalásként értékelt cselekmények között határozott különbségek tehető. Az általa elemzett esetek egy részében a tettes csak felhasználta a számítógép adta lehetőségeket azzal, hogy egy hagyományos bűncselekményt ezen új technikai eszközzel kívánt leplezni. Más esetekben a számítógép programját eleve vagyon elleni bűncselekmény megvalósítása érdekében manipulálta.[163]

Siegler Eszter úgy véli, hogy ha a számítógépes manipuláció során a csalás tényállási elemei is megvalósulnak, akkor ez utóbbi bűncselekményt kell felhívni.[164]

Nézetem szerint, a konkurencia feloldásához a hagyományos csalás tényállási elemeiből kell kiindulnunk. Tradicionálás csalás esetében a sértett "mást", azaz természetes személy lehet. Ez történhet tévedésbe ejtéssel az elkövető által, akár tévedésben tartással más által előidézett megtévesztéssel, amelyet az elkövető kihasznál.

Számítógépet - a büntetőjogban értékelt csalás fogalmát szem előtt tartva - tévedésbe ejteni nem lehet. A számítógép azon program alapján végzi a műveletet, amelyet a számítógépre installáltak, akkor is, ha hiányos vagy téves adatokat táplálnak be, akkor is, ha magát a programot változtatják meg. Az adat- vagy programmanipulációt követően sem a számítógép használójának, sem üzemeltetőjének nincs ráhatása az elektronikus adatfeldolgozásra. E személyek legfeljebb utólag konstatálhatják, hogy vagyoni kár következett be.

Ennek előrebocsátása után, a megoldás "kulcsa" szerintem abban rejlik, hogy sor kerül-e természetes személy megtévesztésére akár adatbeviteli, akár

---

[162] Maurach - Schroeder - Maiwald: Strafrecht. Besonderer Teil. Heidelberg, 1988. s(n) 234-235.
[163] Tóth Mihály: Újabb szempontok a gazdasági bűncselekmények értelmezéséhez. IM Oktatási és Továbbképzési Főosztály, Budapest, 1998. 61.l.
[164] Dr. Siegler Eszter id. mű .... 740.l.

adatfeldolgozási, akár adatkiviteli fázisban vagy sem. Természetes személy gyakorol-e kontrollt az elektronikus adatfeldolgozás folyamata felett, vagy sem. Magam, és ezzel vállalva a dogmatista "megbélyegzést" nem tekintem az elektronikus adatfeldolgozás eredményének utólagos "elfogadását" természetes személy megtévesztésének.

6. 4. Visszaélés bankkártyával

A számítógépes csalások speciális formája a lopott, hamis vagy hamisított bankkártyával történő jogtalan vagyoni haszonszerzés.

A csekk első formája 1416-ban Palermóban jelenik meg. A csekk funkcióit váltják fel a bankkártyák. A készpénz-helyettesítő kártyák közvetlen elődjei az 1920-as években olajvállalatok, szállodaláncok által kiadott plasztiklapok. Az első bankkártyát a Bank of America bocsátja ki 1958-ban, míg Európában az ún. "Karte Blau" A Rotschild-banknál jelenik meg először.[165]

Hazánk pénzügyi történetéből - gazdasági fejletlensége miatt - a "csekk-korszak" kimarad és a fejlett piacgazdaságok technikai evolúciójában a bankkártyák korszakába csöppen. Először 1988-ban jelenik meg az első, ám devizaszámlához kapcsolt, egy évvel később a csekkhez kötött kártya. Ugyanebben az évben kerül forgalomba az első ún. ATM - kártya is.

Ma Magyarországon hárommillió körüli különféle banki műveletek végrehajtására szolgáló bankkártya, valamint nem a bankok által kibocsátott plasztiklapok kerülnek forgalomba, így az American Express (Amex)-kártyái, valamint olajtársaságok üzemanyagkártyái stb.

---

[165] Harsányi Gyöngyi: A bankkártyák, és az alapjukat képező szerződésese viszony sajátosságai. Gazdaság és Jog, 1996. 10. 10-13.l. Dulin Tamás - Kő József: A hitelkártya-visszaélésekről. BSz. 34. 1996. 11.sz. 46 - 50.l.

Dr. Huszti Ernő: Banktan. Budapest, 1996. 125-133.L.

Meir Kohn: Bank- és pénzügyek, pénzügyi piacok. Budapest, 1998. 105-113.l.

A bankkártyák funkciói folyó-számlakezelés, készpénzfelvétel automatából vagy a pénztárból, készpénz nélküli vásárlás, átutalás, vásárlás az Interneten keresztül, hitelfelvétel, csekkgarancia stb. Sőt, - saját tapasztalatból merítve - az Egyesült Királyságban a kártyával történő vásárlás helyén pénzfelvételre is van mód. (Ez az ún. cash - back funkció.) E szolgáltatás hazánkban még ismeretlen.

A legkülönfélébb kereskedelmi, vendéglátó, idegenforgalmi helyek, amelyek vállalják a bankok által kibocsátott kártyák elfogadását az ügyfél számára lehetővé teszik a készpénz nélküli vásárlást vagy szolgáltatás igénybe vételét.

De a nyugat-európai és észak-amerikai országokban plasztiklap jelenti egyben a munkahelyi-, uszoda-, könyvtár-, golf- és jachtklub, stb. belépőt, többféle törzsvásárlói kártyát.

Nagy-Britanniában személyi igazolvány hiányában a bankkártya szolgál az ügyfél azonosítására, míg Franciaországban a csekktömböt garantálja a bankkártya.

Hazánkban 2000. januárjától vezetik be - svájci példa hatására - a személyi igazolványt megtestesítő plasztiklapot.

Nem kicsiny feladatot ró ránk az egyre növekvő számú különböző azonosító (PIN-) kódok megjegyzése. Vagy legalábbis annak azonnali ismerete, hogy hová tehettük azokat.

A bankkártyák számának és a velük végzett műveletek elterjedésével egyidőben a kártyákkal történő visszaélések lehetőségei folyamatosan bővülnek. Ennek megakadályozására szolgálnak a kártyákon szereplő különféle biztonsági megoldások:

- A kártyakibocsátó által használt nemzetközi logo (EC/MC, Visa).
- A kártyán levő dombornyomás és annak valódisága. Több elektronikus kártyán nincs dombornyomás (pl. Cirrus, VISA Electron), legfeljebb a hamisítványokon.
- Bonyolult kártyaszám alkalmazása: meghatározott számkombinációk (bank, ügyfél, kártyatípus stb.) találhatók a kártyákon.

A két legnagyobb kártyatársaság esetében a VISA 4-sel, a Mastercard 5-sel kezdődik. A VISA kártyaszám első négy számjegyét a szám alatt vagy felett

nyomtatva is megismétlik, míg a Mastercardon, a hátlapon, az aláírási panelben is jelzi a kártyaszámot.

- Hologramos jelek alkalmazása.
- Csak uv-lámpával látható jelzések.
- A megjelölt lejárati dátum megakadályozza, hogy a kártyát érvényességi idején túl is használják.
- A kártya hátoldalán szereplő aláírás.

A kereskedelmi és vendéglátó helyeken történt vásárláskor a kártyabirtokos aláírásával hitelesíti a kártyával történő vásárlást. Vajon ellenőrzik-e minden esetben a kereskedők az aláírást, és ki tudják-e szűrni a hamis aláírásokat?

A kártyaelfogadással összefüggő technikai eszközök:

1. Kézi lehúzó (imprinter): Kereskedelmi egységekben történő vásárláskor a kártyakibocsátó bankkal szerződésben álló kereskedő a vevőtől átveszi a dombornyomásos kártyát, és azt a "kézi lehúzón" áthúzza. Ez az eszköz azonosítja az ügyfelet, valamint az általa használt kártyát és egy bizonylaton, amelyet az ügyfélnek alá kell írnia, megjeleníti a banktól, majd igényelhető összeget. A bizonylatokat kereskedő összegyűjti, és a bankhoz továbbítja.

Ez a módszer lassú és többféle visszaélés forrása lehet.

Hetek is eltelhetnek mire a kereskedő a bankhoz benyújtja az összegyűjtött bizonylatokat, ami alapján a bank csak ezen idő elteltével tájékozódhat arról, hogy túllépték-e a kártyatulajdonos számára nyitva álló összeget.

A kereskedő is csak hosszú idő után kaphat értesítést a letiltott (ellopott vagy elvesztett) kártyák listájáról. Ami esetleg több száz oldalas, amelyet át kell böngésznie.

Kézi lehúzó eszközök száma - a technika fejlődése, és a visszaélések könnyebb megvalósítása miatt - csökken.

2. Elektronikus terminal (POS): Ez egy olyan készülék, amely a kereskedelmi egységben levő elektronikus (telefon- vagy más adatátviteli) vonalon tartja a

kapcsolatot a kártyát kibocsátó központtal. Korábban működnek off-line terminálok is, de ezek száma egyre csökken. A kereskedő a kártyát a készülékbe helyezi és a vásárlás ellenértékét azonnal levonja az ügyfél számlájáról. E készülékek nemcsak az ügyfelet ellenőrzik, hanem a letiltott kártyák listájával is összevetik a használt kártyát. A kereskedő feladata mindössze a bankkártyán levő aláírás összevetése az ügyfél bizonylaton történő aláírásával.

3. Bankjegykiadó automata (ATM: Automated Teller Machine): a bankkártyával ezen terminálokból készpénz vehető fel és elterjedőben vannak azok az automaták, amelyek pénzbefizetést teszik lehetővé. Lopott vagy hamisított bankkártyával eszközölt jogosulatlan pénzszerzést az ún. PIN-kód nehezíti meg. Az automaták általában háromszor, esetleg négyszer végrehajtott eredménytelen "kísérletezgetés" után a kártyát bevonják. A bankautomatákat már drága videokamerákkal is felszerelik, amely rögzíti az ügyfelek pénzkivételeit és befizetéseit. (Ezt takarják le egy szövettel, pl. pulóverrel, kabáttal.)

Az ATM-ból eszközölt készpénzfelvételhez a kártya és a PIN-kód egyidejű ismerete szükséges. A PIN-kód jogtalan megszerzésének alábbi formáit ismerhettük meg:

A. Az ATM billentyűzetére tett műanyag fólián rögzíthető az ügyfél ujjnyomata. Ezután már "csak" a bankkártyát szükséges - bármilyen eszközzel, és módon pl. zsebtolvajlás útján avagy erőszakkal, fenyegetéssel - megszerezni. Majd a PIN - kód ismeretében könnyedén "leemelhető" a kártyaszámlán szereplő összeg. Nem árt a kártyahasználat előtt az automata billentyűzetére is pillantást vetnünk, mielőtt a műveletet elkezdenénk.

Ennek vagy bármely más módon történő nyomrögzítés megakadályozására alkalmazzák néhány pénzintézetnél az ún. vandálajtót, amely csak a kártya behelyezésekor emelkedik fel, és a kártya elvételével záródik ismét.

B. Bankkártya, és PIN-kód megszerzése kényszerrel: bármilyen technikai eszköz és megoldás is védi a bankkártyáinkat, a pénzügyi műveleteket, kivédhetetlen támadás érheti a kártyabirtokost, ha az elkövetők a pénzfelvétel során vagy azt közvetően erőszakkal vagy fenyegetéssel szerzik meg a bankkártyát és a hozzátartozó PIN-kódot.

A kártyabirtokosok is tehetnek PIN-kódjuk védelmében, ha nem tartanák ezt a fontos számot a kártyára felírva vagy a pénztárcájukban, noteszukban stb. és figyelmeztetnék az automatánál sorban mögöttük állókat bizonyos távolságtartásra. A szó igazi értelmében túl sokba kerülhet az ügyfél hanyagsága, ha a kártyáját ott felejti a gépbe és elrohan a kivett pénzzel.

A bankkártyákkal kapcsolatos visszaélések több formája vált már ismertté:

1. A k á r t y a - k i b o c s á t á s k o r megvalósítható visszaélések:

1.1. jogosulatlan kártyához juttatás (scoring csalás): olyan személy számára juttatnak kártyát, aki nem jogosult használatára vagy kisebb összegű hitelkártyára jogosult.

Magyarországon még nem terjedtek el az igazi hitelkártyák, így ezen visszaélési forma nem jellemző.

1.2. Információk jogosulatlan kiszolgáltatása: ügyfelek adatainak (kártyaszámának és/vagy PIN-kódjának) a kiszolgáltatása, amelyek banktitoknak minősülnek. Ezen adatok segítségével készíthető hamis kártya. Vagy a másik tipikussá váló visszaélés során, pl. a zsebtolvajokkal "ellopatott" kártyához a PIN-kód megszerzése. Ez utóbbi megakadályozására szolgál a kártya letiltás lehetősége. A nyomozás során tisztáznia kell, hogy a bankon belül ki, és milyen ismeretekkel bírt a kártyákkal összefüggő információkkal. Ez segíti a gyanúsítottak körének szűkítését.

1.3. Lejárt kártyák újrahasznosítása: a kártyákat a bankok évente-kétévente bevonják, majd jogszabály által előírt rendelkezések szerint meg kell semmisíteni. A kártyán levő mágnesszalagon levő lejárat éven módosítva adott egy "új" kártya.

Sajnos, a bankok nem mindig módosítják az új kártya átadásával a PIN-kódot. Ez is egy veszélyforrás.

1.4. Át nem vett kártyákkal történő visszaélés: a bank értesíti ügyfelét, amikor megérkezik hozzá a kártya és a lezárt borítékban a PIN-kód. Ennek jogosulatlan megismerésével a kártya használhatóvá válik.

2. A kártya-felhasználás során megvalósítható visszaélések:

2.1. A kártyabirtokos visszaélései:

2.1.1. Hamis adatokkal történő kártyaigénylés: bankkártya igénylés során adatlapot kell kitölteni, amelyek egy részét a banki alkalmazott ellenőrzi, míg másokról "büntetőjogi felelősségünk tudatában kell nyilatkozni". A bank ellenőrzési és elfogadási mechanizmusai szolgálnak ennek kiszűrésére.

2.1.2. Saját kártyával történő fedezettúllépés: a kártyabirtokos szándékosan többet költ, mint amennyi a kártyaszámláján van. Csak off-line terminálon keresztül történő vásárlásnál valósítható meg.

2.2. Más kártyájával megvalósítható visszaélések:

2.2.1. Elveszett vagy lopott kártyák használata: az elhagyott vagy ellopott kártyával a PIN-kód hiányában is lehetőség van a kártyával történő vásárlásra, még azelőtt, mielőtt a kártyabirtokos bejelentését követően a bank azt letiltja.

2.2.2. Az ügyfél által át nem vett kártyákkal történő visszaélés. Az 1.4. esettől eltérően ebben az esetben postai úton történik a kártyák kiküldése a kártyabirtokosnak. Mindenképpen el kell érni a kártya bankban történő átvételének kötelezővé tételét.

2.2.3. Hamis vagy hamisított kártyák használata esetén egy már létező kártyáról készítenek az elkövetők másolatot, "klónozzák" azt ellopását követően vagy a banktól történő átvétele előtt.

3. A bankkártya elfogadása során megvalósítható visszaélések:

3.1. "Ál" üzletnyitás. Az elkövetők hamis, hamisított okiratokkal olyan kereskedelmi üzletet nyitnak, amelyek bankokkal szerződést kötnek kártyaelfogadásra. Néhány heti vagy havi forgalom után, bevárva a banktól átutalt összegeket az álkereskedők megszüntetik vállalkozásukat.

3.2. "Csalárd összejátszás" a jogosulatlan vásárlókkal: a "kereskedő" szándékosan tud arról, hogy hamis, hamisított vagy lopott kártyát használnak fel, elfogadja azt és igazolja a vásárlást.

3.3. A kártyalehúzások megtöbbszörözése. Ebben az esetben "fizetéskor" a vásárolt összeg többszörösével terheli meg a vevő kártyaszámláját.

4. A bankjegykiadó-automata (ATM) felhasználásával elkövetett bankkártya visszaélések

4.1. Az ATM pénzkiadó nyílásának leragasztásával: az elkövetők az ATM pénzkiadó nyílását mindkét oldalán ragacsos szalaggal ragasztják le. A kártyabirtokos miután beüti PIN-kódját, és kijelöli a végrehajtandó műveletet az automata nem ad ki bankjegyeket, mert azok a pénzkiadó nyílásában felragadnak a ragasztós szalagra és ott maradnak. A jogosan méltatlankodó ügyfél segítségére siet a helyszínen tartózkodó elkövető.

4.2. "Ál-ATM" - telepítésével az elkövetők egy megtévesztésig hasonló ATM-et telepítenek valamely közterületen, esetleg másutt. Az ügyfél begépeli PIN-kódját, kijelöli a végrehajtandó műveletet, majd az automata képernyőjén olyasféle üzenet lesz olvasható, hogy a "kártyája lejárt", "túllépte a számára engedélyezett keretet", vagy "nem jogosult erre a műveletre" stb. és ezzel a bankkártyát nem adja vissza, visszatartja azt. Az elkövetők számára adott egy bankkártya és a hozzátartozó PIN-kód. [166]

---

[166] Dulin Tamás - Kő József: ... id. mű 53-58.l.
Dr. Nagy Zoltán: A bankkártyával összefüggő visszaélések. Jura 4. 1997.2. 11-15.l.

A bankautomaták elleni bűncselekmények elnevezése a szakirodalomban **CD-CRIME** (Cash Dispenser - Crime), azaz a pénzkiadó automatával összefüggő bűncselekmények.[167]

E magatartások minősítése a büntetőjog tradicionális törvényi tényállásai alapján nem mindenütt lehetséges.

Az elkövető által lopott vagy hamisított bankkártyával bankautomatán keresztül végrehajtott pénzátutalást Japánban nem minősítik bűncselekménynek. E távoli országban "európai füllel" is jól érthetően indokolták meg az ítéletet. Mivel a lopás tényállási eleme csak "testet öltött" ingó dolog lehet, így a pénzátutalás, mivel pénzkivételre nem kerül sor, lopásként nem értékelhető, legfeljebb, ha bankalkalmazott követte el hivatali visszaélésnek (japán Btk. 247. §).[168]

Eltérő a büntetőjogi minősítés, ha a bankautomatából jogosulatlanul történt a pénzkivétel. Az elkövető ekkor nem a saját nevére szóló, hanem hamisított vagy lopott bankkártyával szerez készpénzt, tehát megtévesztő magatartásának eredményeképpen kíván jogellenes vagyoni előnyhöz jutni. A csalás megállapítását azonban az akadályozza, hogy az elkövető nem természetes személyt tévesztett meg. Ennek hiányában lopást állapítanak meg Németországban, Ausztriában, Spanyolországban, Hollandiában, Görögországban, Japánban.[169] Bár Hollandiában egyes alsóbb fokú bíróságok ezt a magatartást hamis kulccsal elkövetett lopásnak ítélik, de a Legfelsőbb Bíróság ezt a vélekedést nem osztja.[170]

Nem kevés dilemmát okoz annak a megítélése, hogy a saját bankkártyával történő visszaélés (pl. a hitelkeret csalárd, fraus civilisként értékelhető túllépése) büntetőjogi felelősségre vonást keletkeztessen-e vagy sem. A francia Cour de Cassation a civiljogba vonja ezt a kérdést. Ítéletének summázata az, hogy a "szerződésben foglalt feltételek megváltoztatása nem vonhat maga után represszív szankciót."[171]

---

[167] Revue ..... p. 435.
[168] Revue ..... p. 439.
[169] Revue ..... p. 154., p. 569., p. 479., p. 368.
[170] Revue ..... p. 479.
[171] CE Recommendation (89) 9. ..... p. 38.

Erre a véleményre, valamint arra alapozva, hogy az Egyesült Államokban "A hitelkártya csalásról" 1984-ben született törvény mellőzte e cselekmények büntetőjogi üldözését az ET. (89) 9. sz. Ajánlása sem számol a saját kártyával való visszaélés kriminalizációjával. Igaz, hogy a nyolcvanas évek közepén - végén a bankkártya forgalom nem számottevő.

Ezzel ellentétes a finn Btk., amely 1991-től bünteti a saját kártyával való visszaélést, igaz fenntartva a késedelem nélküli kompenzáció lehetőségét a büntetlenül maradáshoz.

A bankkártyával való visszaélés kriminalizációja a nemzetközi törvényhozásban új keletű jelenség.

1. Egyes országokban nem alkotnak önálló törvényi tényállást e bűncselekmény büntetni rendelése céljából, hanem a már kodifikált számítógépes csalás esetei közé sorolják, mint tipikus in-put manipulációt. Idetartozik a számítógépes bűncselekményeket a nyolcvanas évek utolsó harmadában kodifikáló országokra, így **Németországban, Ausztriában, Görögországban,** és **Japánban**. De Ausztriában vitatott e törvényi tényállás feltétlen alkalmazhatósága, mivel a más nevére szóló bankkártyán feltüntetett adatok a számítógép számára "helyesek" és "hiánytalanok". E vélekedés alapján a magatartás lopás értékelendő. [172]

2. **Hollandiában** a bankautomatából eszközölt lopott vagy hamisított bankkártyával végrehajtott jogosulatlan pénzkivételt a holland Btk. 310. §-ban szabályozott tradicionális lopásként értékelik.[173]

3. **Franciaországban** a cselekményt csalárd módon elkövetett lopásnak minősül. (Code Penal 379. §-a). [174]

4. Azon országok, amelyek a számítógépes manipulációkat a kilencvenes évek elején kriminalizálják, e mellé önálló törvényi tényállásba veszik fel a bankkártyával visszaélést. **Finnországban** bár a számítógépes csalás meghatározása szűkszavú, de a bankkártyával visszaélés definíciója rendkívül részletező:

---

[172] Revue ..... p. 155.
[173] Revue ..... p. 479.
[174] Revue ..... p. 301.

"Módosító novella 37. §: aki abból a célból, hogy magának vagy másnak vagyoni előnyt szerezzen

1. bankkártyát, fizetési kártyát, hitelkártyát, csekket vagy más hasonló fizetési eszközt tulajdonosának hozzájárulása nélkül illetve a tulajdonostól kapott megbízás túllépésével, vagy jogtalan módon használ, avagy

2. átutalást végez ilyen fizetési eszközzel vagy ilyen utánzattal két évig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő.

Az előző szakasz szerint büntetendő az a személy is, aki mértéktelenül túllépi számlája egyenlegét, kimeríti hitelkeretét, vagy más módon visszaél fizetési eszközével, és ezzel kárt okoz, kivéve, ha a kárt késedelem nélkül megtéríti." [175]

Svájcban is a bankkártyával való visszaélés külön törvényi tényállásban lelhető fel.

"148. § (1) Az a fizetésképtelen vagy fizetni nem tudó személy, aki csekk- és hitelkártyájával vagy hasonló fizetési eszközzel visszaél, illetve a vagyoni értékű szolgáltatást megszerez, és ezzel kárt okoz öt évig terjedő börtönbüntetéssel sújtható.

(2) A büntetés tíz évig terjedő fegyház- vagy börtönbüntetés, ha a bűncselekményt üzletszerűen követik el." [176]

A bankkártyával visszaélés szabályozása új keletű, ám néhány **tanulság** azért adódik:

1. nem minden ország szabályozza külön a bankkártyával visszaélést. Németországban, Ausztriában "számítógépes csalásnak" minősül: in-put csalásként értékelik, mivel a kártyát használó nem jogszerű a birtokos, tehát ez jelenti a cselekmény megtévesztő jellegét.

---

[175] Centenary of the Finnish Penal Law ... id. kiadvány (v.ö. 97.) p. 18. - saját fordítás

[176] www.gesetze.ch/sr/311.0/311.0_012.htm

Hollandiában, Franciaországban "csalárd módon megvalósított lopásként" értékelik ezt a bűncselekményt.

2. Az elkövetési magatartások a bankkártya jogosulatlan használata, amely a kártyabirtokos hozzájárulása nélkül vagy a hozzájárulás kereteit túllépve követik el. Minden bizonnyal a bankkártya használatának bővülésével újabb és újabb magatartások válnak ismertté.

3. A tényállások eredményt is meghatároznak, ez pedig e visszaéléssel okozott kár.

Hazánkban nem kevés fejtörést okozott volna az 1994-es törvénymódosítást megelőző, a hazai kriminalisztika történetében első, de az eddig ismert legnagyobb (?) kárt okozó ilyen jellegű bűncselekmény minősítése.

1992. tavasza óta folyik nyomozás ismeretlen elkövető(k) ellen, aki(k) egy hónap alatt 1.583 esetben vesz(nek) fel 20.000.- ft-ot az egyik hazai pénzintézet (OTP) pénzkiadó automatáiból. Az okozott kár 31.660.000.- ft. (!), ami tisztes tanulópénznek tekinthető.

Az elkövető(k) egy talált vagy lopott személyi igazolvánnyal folyószámla-szerződést köt(nek) a pénzintézettel, aminek révén egy bankkártyához jut(nak). Ezt követően lopott vagy külföldről becsempészett ún. nyers, tehát csupán mágnescsíkokkal ellátott, viszont semmilyen információt sem tartalmazó kártyákra rámásolja vagy rámásolják a legális bankkártyáról a szükséges információkat.

A hazai pénzintézet off-line rendszerű bankautomákat üzemeltetett, amely a pénzforgalmat lemezre rögzítette, amiket meghatározott időközökben vittek el és futtatták le a központi számítógépeken. Ez a technikai megoldás az elkövető(k) kezére játszik, hiszen a lemez ellenőrzése, lefuttatása közötti időben a bankautomaták forgalmát nem regisztrálták. Az automaták akkor hetente egyszer tettek lehetővé 20.000.- ft. kivételét. Az ismeretlen elkövető(k) túljár(nak) az automata rendszerén, amely egy apró elektronikus jellel látja el a kártyát, ami lehetetleníti, hogy azt egy héten belül ismételten használhassák. [177]

---

[177] Magyar nemzeti jelentés. Kézirat, készült az 1992-es würzburgi AIDP Kollokviumra 4.1. (Készítették Dr. Kertész Imre és Dr. Pusztai László). Angol nyelven Revue ... p. 375.,

A cselekmény büntetőjogi minősítése kapcsán a fondorlatos elkövetés alapot adhatott volna arra, hogy a csalás törvényi tényállása jöhetett volna szóba.

Az előzőekből látható, hogy a csalás bűncselekményének megállapításához az szükséges, hogy a sértett téves tudatában akár személyesen, akár a vagyoni viszonyaiban rendelkezésre jogosult diszponáljon. Ez a vagyoni intézkedés e körben is hiányzik, ugyanis az elszenvedett kár tulajdonképpen a bankautomata programjától függ, amely limitálja az egyszeri alkalommal felvehető pénzösszeg nagyságát.

A lopott vagy hamisított bankkártyával eszközölt jogosulatlan pénzszerzés tehát csalásnak nem minősülhetett volna, éppen a passzív alany vagyoni jellegű rendelkezésének kizártsága miatt. Szóba jöhetett volna akkoriban a Btk. 316. szakaszában meghatározott lopás bűncselekménye. A lopás megállapításához elegendő az idegen, ingó és értékkel bíró dolog jogtalan eltulajdonítás végett történő megszerzése. Legfeljebb hiányérzetünk támadhatott volna abból, hogy itt a lopás csalárd módon valósult meg. A törvény-előkészítés során a bankkártyával visszaélés bűncselekményét önálló törvényi tényállásban kívánják kriminalizálni, elejét véve az esetlegesen felmerülő értelmezési vitáknak, vagyis tekinthető-e ez a cselekmény in - put (beviteli szakban elkövetett) manipulációnak vagy lopásnak.

Alternatív tervezet kerül a törvényhozó elé. Az egyik változatban ez a bűncselekmény egy önálló törvényi tényállásban jelent meg, míg másik megoldásként a bűncselekmény a lopás minősített eseteként szerepelt.[178] A

---

[178] Büntetőjogi és Kegyelmi Ügyosztály 35.135/1992. IM. III. 23. §-ában a bankkártyával visszaélés *"A"* változata az alábbi:
"(1) A Btk. 316. § (2) bekezdése a következő k) ponttal egészül ki:
k) hamis vagy hamisított bankkártya felhasználásával (követik el)
(2) A Btk. 316. (4) bekezdésének 1. pontja helyébe a következő rendelkezés lép:
1. a (2) bekezdés a/ - d/ és k/ pontjában meghatározott módon,
(3) A Btk. 316. § (5) bekezdésének b/ pontja helyébe a következő rendelkezés lép:
b) a nagyobb értékre elkövetett lopást a (2) bekezdés a/ - d/ és k/ pontjában meghatározott módon.
(4) A Btk. 316. § (6) bekezdésének b/ pontja helyébe a következő rendelkezés lép:
b) a jelentős értékre elkövetett lopást a (2) bekezdés a/ - d/ és k/ pontjában meghatározott módon"

törvényhozó az előbbi megoldást választja. A bankkártyával visszaélés deliktuma nem a vagyoni, hanem eléggé vitathatóan a gazdasági bűncselekmények közé került.

Az 1994-től hatályos büntetőjogi rendelkezést, 1998-ban egészítik ki további elkövetési magatartásokkal az alábbi tényállás (1) bekezdés b. és c. pontjaival, majd 1999-ben újabb kárértékkel bővül a tényállás.

"313\C. § (1) Aki

a./ hamis vagy meghamisított bankkártyát jogtalan haszonszerzés végett felhasznál

b./ bankkártyát jogosulatlanul felhasznál,

c./ a hamis, a hamisított vagy a jogosulatlanul használt bankkártyával történő fizetést elfogadja,

és ezzel kárt okoz, bankkártyával visszaélést követ el.

(2) A büntetés vétség miatt két évig terjedő szabadságvesztés, közérdekű munka vagy pénzbüntetés, ha a bankkártyával visszaélés

kisebb kárt okoz vagy a bűncselekményi értékhatárt meg nem haladó kárt okozó bankkártyával visszaélést

a./ bűnszövetségben,

b./ üzletszerűen

követik el.

(3) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha

a./ a bankkártyával visszaélés nagyobb kárt okoz,

b./ a kisebb kárt okozó bankkártyával visszaélést a (2) bekezdés

a./ - b./ pontjában meghatározott módon követik el.

(4) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha

a/ a bankkártyával visszaélés jelentős kárt okoz,

b./ a nagyobb kárt okozó bankkártyával visszaélést a (2) bekezdés a./ - b./ pontjában meghatározott módon követik el.

(5) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha

a./ a bankkártyával visszaélés különösen nagy kárt okoz,

b./ a jelentős kárt okozó bankkártyával visszaélést a (2) bekezdés a./ - b./ pontjában meghatározott módon követik el.

(6) a büntetés öt évtől tíz évig terjedő szabadságvesztés, ha

a./ a bankkártyával visszaélés különösen jelentős kárt okoz,

b./ a különösen nagy kárt okozó bankkártyával visszaélést a (2) bekezdés a./ - b./ meghatározott módon követi el.

(7) A (2) - (5) bekezdés szerint büntetendő az is, aki a visszaélés bankkártyával bűncselekményét a csekkgarantáló kártyához tartozó csekkre nézve követik el.

313/D. szakasz A 313/B. - 313/C. szakasz alkalmazásában bankkártya minden olyan, pénzintézeti tevékenységet végző jogi személy által kibocsátott kártya, amely pénz felvételére, illetőleg áru vagy szolgáltatás ellenértékének kiegyenlítésére szolgál."

A bűncselekmény tárgyának taglalása kapcsán különbséget kell tennünk a jogi és az elkövetési tárgy között.

Az előbbiről megállapíthatjuk, hogy a bűncselekmény bár a gazdasági deliktumok között szerepel, valójában olyan vagyoni viszonyokat sért. Szerződés alapján jönnek létre a pénzintézet és az ügyfelek illetve, azon kereskedelmi, vendéglátó idegenforgalmi és más cégek között, amelyek a bankkártyák elfogadását vállalják. Ezeket a szerződéses viszonyokat bankkártyák testesítik meg. A bankkártya a bank tulajdona marad, a meghatározott időre, általában egy vagy két évre szóló szerződéssel a számlatulajdonos a kártya jogszerű használója lesz. A bankkártyával való visszaélés a két fél közötti vagyoni viszonyok sérülnek. Ez alapján a bankkártyával visszaélés bűncselekményének rendszerbeli helye - de lege ferenda - a vagyon elleni bűncselekmények között van helye.

A bűncselekmény tárgyi oldalának szereplő elkövetési magatartás a jogosulatlan visszaélés a kártyák funkciói által biztosított lehetőségekkel:

a. Hamis vagy hamisított bankkártyát jogtalan haszonszerzés végett felhasznál:

- létező bankkártyáról készített hamis kártyával (üres plasztiklapra, lejárt kártyára stb.) való vásárlás vagy ATM-ből történő pénzkivétel.
- bankkártya dombornyomásának kivasalása és újra nyomása.

b. Bankkártyát jogosulatlanul felhasznál:

- a kártyabirtokos túllépi a számára nyitva álló hitelkeretet,
- elvesztett vagy lopott kártya használata,
- át nem vett kártyákkal való visszaélés (akár bankon, akár a postai kézbesítés során történt jogellenes megszerzést követően),
- idevehetjük az esetet, amikor a kereskedő többször lehúzza a kártyát (majd ezt igazoltatja a kártyabirtokossal).

c. Hamis, hamisított vagy a jogosulatlanul használt bankkártyával történő fizetést elfogadja.

A bűncselekmény aktív alanya bárki lehet. Az elkövetési magatartástól függően akár a kártyabirtokos pl. a (2) bekezdés, vagy a kereskedő a (3) bekezdés megvalósításánál. A számlatulajdonos rendelkezési jogot engedhet más (pl. a társkártyabirtokos) számára.

A bűnösség értékelésénél megállapítható, hogy az elkövető magatartása az (1) *a.* pontjában meghatározott elkövetés esetében célzatos. Tehát azért él vissza lopott, hamis, hamisított kártyával, hogy ezen kártyák segítségével jogtalan vagyoni haszonra tegyen szert. A célzat az egyenes szándékot (dolus directus) alapozza meg. A *b.* és a *c.* pontban írt magatartás a szándékosság mindkét formájával (egyenes és eshetőleges szándékkal is) megvalósítható. Nem szükséges célzat, de a bankkártyával történő visszaélés, valamint a hamis stb. bankkártyák elfogadása szintén vagyoni haszonra való törekvést feltételez.

A bűncselekmény tárgyi elemei között kiemelendő a kár, amely a büntetőjogban a vagyonban ténylegesen okozott értékcsökkenés. Ehelyütt a jogosulatlanul felvett pénz összege valamint a jogosulatlanul vásárolt áru vagy az igénybe vett szolgáltatás ellenértéke lehet. A bankkártyával való visszaélés bűncselekményének nincs szabálysértési alakzata. A szabálysértési értékre (10 ezer ft.-ig) elkövetett visszaélés csak akkor bűncselekmény, ha azt üzletszerűen vagy bűnszövetségben valósítják meg.

A minősített esetek részben a kárérték, részben a "bűnszövetség" és az "üzletszerűség" minősítő körülmények alapján épülnek fel: kisebb érték: 10 ezer forinttól 200 ezer forintig, a nagyobb kár: 200 ezer forint feletti összegtől 2 millió forintig, a jelentős érték: 2 millió feletti összegtől 50 millió forintig, a különösen nagy érték: a 50 millió forint felett összegtől 500 millió forintig terjed, míg a különösen jelentős, ha 500.000.000.- ft. feletti összeg (Btk. 138/A. §).

Felvetődik a kérdés, hogy vajon egy *bankkártya jogtalan eltulajdonítása* hogyan értékelendő? E kérdésre a választ a Legfelsőbb Bíróság adja meg, amikor iránymutató ítéletében kifejti "a Btk. 333. § 1. pontjában meghatározott értelmező rendelkezés szerint dolognak tekintendő a vagyon jogosultságot megtestesítő okirat, amely a benne tanúsított vagyon érték vagy jogosultság feletti rendelkezést önmagában biztosítja. Az ilyen okiratok bemutatóra szólnak, az a személy rendelkezhet velük, akinek az okirat a birtokában és nem vizsgálható a tényleges tulajdonos kiléte. .....a bankkártya okiratnak nem tekinthető, ugyanakkor a gyakorlati életben a fenntartásos takarékbetétkönyvhöz hasonló elbírálás alá esik, mivel a bankkártya birtoklása önmagában nem teszi lehetővé a pénzhez való hozzájutást, illetve az áru vagy szolgáltatás megvásárlását." A Legfelső Bíróság ítéletében kitér a továbbiakban arra, hogy a bankkártya használatához PIN-kód vagy aláírás szükségeltetik, így önmagában a bankkártya lopás tárgya nem lehet.[179]

A bankkártyával visszaélés kísérleti szakba azáltal jut, ha az elkövető az ATM-be helyezve a kártyát, a hozzátartozó PIN-kód (akár helyes, akár helytelen) első számjegyét leütötte.

Ha a bűncselekmény még korábbi stádiumait tekintjük, akkor egy másik tényállás felé kell fordulnunk. Ugyanis a 313/B. § a bankkártya-hamisításról nem más, mint delictum sui generis előkészület.

A bankkártyával visszaélések visszaszorításáért, mind a kártyakibocsátóknak, mind a bankoknak, mind a kártyabirtokosoknak a biztonságos kártyaforgalom lebonyolítása céljából tenniük kell. Közösek az érdekeink!

6. 5. A vagyoni jogosultságokat sértő "adatlopás"

A vagyoni jogokat, követeléseket megjelenítő számítógépes adatállományok módosítása, "megcsapolása" nemcsak fraudulens módon történhet, hanem csalárdság hiányában is.

Ez a magatartás jogellenes vagyoncsökkenést idéz elő a sértett vagyoni viszonyaiban jogellenes vagyoncsökkenést és az elkövetőnél szintén jogellenes - vagyongyarapodást idéz elő.

Az elkövető azért módosítja (törli, írja felül, kiegészíti) az adatállományt, hogy az adatokban kifejeződő, a sértett vagyoni jogosultságait elvonja, azért, hogy azzal sajátjaként rendelkezzen. A tevékenység tehát strukturálisan a lopásban szabályozott magatartásával egyező, azaz egy újabb hagyományos bűncselekmény, amely a technikai fejlődésével újabb elkövetési eszközzel gazdagodik.

A lopás elkövetési tárgya az ókortól a XIX. század utolsó harmadáig csak idegen, ingó és értéket képviselő dolog lehetett: "Res quae tangi possunt", vagyis olyan dolog, ami birtokba vehető, vagyis kézzelfogható, látható stb. Már a villamos munka jogtalan elsajátításának lopásként való értékelése igen élénk irodalmi vitát váltott ki a magyar és a német büntetőjog-tudományban. Olyan kiemelkedő német kriminalisták helyezkednek a lopás tárgyaként történő elismerése ellen, mint Franz von Liszt vagy Karl Binding.[180] Bár az 1878:V. tc. a Csemegi-kódex hatálybalépését követően a Curia ítélkezési gyakorlatában kiterjeszti a "testi tárgy" fogalmát a villamos áramra is.[181] Az 1907:III. tc. (A hazai ipar fejlesztéséről) - amely az 1900-as német törvényt véve példának - a villamos áramot helyezi büntetőjogi védelem alá (2. § (3) bekezdés).

---

[179] BH 1999/57.sz.

[180] idézi Dr. Finkey Ferenc: A magyar büntetőjog tankönyve. Budapest 1914. 696 - 697.l.

[181] Dr. Angyal Pál: A lopás ... id. mű 25.l.

Míg a XX. század kezdetekor a villamos energiát veszik fel a lopás elkövetési tárgyai közé, addig a XX. század végén az ún. "dematerializált értékpapír" fogalmával bővült az elkövetési tárgyainak köre. Ezt nevezhetjük a lopás atipikus tevékenységi tárgyának. Atipikus, mivel az elektronikus adat nem látható, nem érinthető, és további technikai eszközök segítségével válik csak érzékelhetővé. Az 1998. évi LXXXVII. tv. 79. § egészíti ki a Btk. 333. § értelmező rendelkezéseinek 1. pontját a "dematerializált formában kibocsátott értékpapírral". A magyar Értékpapír törvény 1998. július 1-től teszi lehetővé azt, hogy az értékpapírt kibocsátó gazdasági társaságok értékpapírjaikat fizikai léttel bíró papír vagy dematerializált formában bocsáthassák ki. Ez utóbbi esetben a befektető által vásárolt értékpapír csak értékpapírszámla-követelés formájában létezik. A befektetők egy letéti igazolást kapnak a brókercégtől, míg az értékpapírokat értékükkel, befektetőjük azonosításával elektronikus adat formájában jelenik meg a számítógépen. A dematerializált értékpapírok forgalma a számítógépes hálózatokon keresztül folyik. "A német terminológia ezeket a papírtalan értékpapírokat értékjognak (Wertrecht) nevezi."[182] **Szécsényi László** szerint az "értékadat kifejezést kellene elfogadni az értékjog kifejezés helyett, amely a jog különleges rögzítésének módjára utal".[183] Tehát 1999. március 1-től ezen adatok "el...-donítása" lopásnak (Btk. 316. §) minősül. Az értékpapírok megjelenítésére szolgáló adatsor egészét vagy annak egy részét törlik az adott állományból és megjelenítik egy másik állományban.

A lopás bűncselekményének minősítését az okozott kár mértéke határozza meg. Befejezett bűncselekmény esetében az okozott kár mértékének a megállapítása nem idéz elő problémát, ám kísérlet esetében az elkövető szándékának bizonyítása nem kevés nehézséget vethet fel. Bár hatályos tényállás minősítő körülményei között nem szerepel a hacking, ám - ha ez büntetni rendelt lesz - a bíróságnak súlyosító körülményként kell majdan figyelembe venni, ha az elkövető védett számítástechnikai rendszerbe jogosulatlanul belépve követi el az "adatlopást".

---

[182] Dr. Szécsényi László: Gazdaság és Jog, 5. 1997/10. 8 - 9.l.
[183] Dr. Szécsényi László: id. mű ..... 8 - 9.l.

6. 6. Az elektronikus adatfeldolgozás- és adatátvitel akadályoztatása

Az informatizált társadalmi tevékenységet érzékenyen érinti az elektronikus adatfeldolgozási- és adatátviteli rendszerek akadályoztatása, különösen e rendszerekben történő károkozás.

Az akadályoztatásról csak abban az esetben beszélhetünk, ha az a számítástechnikai rendszer működésének megnehezítését vagy meghiúsítását öleli fel. Tehát ki kell zárnunk a számítógép-kezelő(k) elleni erőszakot vagy fenyegetést.

Az akadályoztatás legáltalánosabb formája a károkozás, amely irányulhat a rendszer technikai eszközei (a hardver), az adathordozók (mint fizikai léttel bíró dolgok) ellen, továbbá a rendszert vezérlő programok, programrendszerek (a szoftver) valamint a számítástechnikai rendszerekben feldolgozott vagy tárolt adatok (ez utóbbiak, mint testetlen dolgok) ellen.

A téma tárgyalása e tagolás mentén történik, azonban hangsúlyozni kell, hogy ez a felosztás csupán didaktikai célokat szolgál. Hiszen pl. a hardver és a szoftver elleni támadások közötti különbségtétel viszonylagos, mivel az operációs rendszert akár egy chipbe is beépíthetnek.

A károkozó magatartások változatos formát ölthetnek. Itt említhetjük többek között a fizikai rongálást, az adatok jogellenes törlését, továbbá az új típusú vírusprogramokat.

Emiatt a potenciális kár vagy veszteség mértéke is széles skálát fog át: a minimális kártól a rendkívül tetemes, netán a pótolhatatlan veszteségig. Ez előbbire szolgálhat például egy olyan vírusprogram, amely az adatállományt összekeveri, amelyet azonban visszarendezhet egy helyreállító- (service-) program hosszabb - rövidebb idő alatt. Míg az utóbb esetre említhetjük a számítástechnikai rendszer fizikai megsemmisítését vagy azon adatállomány elpusztítását, amelyhez az adatgyűjtés a korábbi feltételek közepette megismételhetetlen.

A károkozásban megnyilvánuló elhatározás is sokrétű lehet, hiszen ez a rongálás elemi szándékától a rendszert megbénítani kívánó szabotázs szándékáig, sőt a terrorcselekmény céljáig is terjedhet. A károkozó magatartás tipikus formája a *rongálás*.

Más vagyonának jogellenes megrongálása (damnum iniuria datum) civiljogi és büntetőjogi felelősségre vonást egyaránt eredményezhet. A nemzetközi judikatúrában a kriminalizáció a civiljogi védelmet erősíti azzal, hogy a szándékosan elkövetett és meghatározott kárértéket meghaladó rongálást kriminalizálására került sor.

A vagyontárgyak büntetőjogi védelme - amely a közveszélyt előidéző rongálás esetét kivéve - relatíve későn, a XIX. század elejétől válik általánossá és ezek a dolgokban testet öltött vagyoni tárgyakra terjed ki.

A büntető törvénykönyvekben a rongálás minősítését általánosan a vagyontárgy értéke és jellege határozza meg. Ez utóbbi azt jelenti, hogy lehetséges a dolognak speciális, büntetőjogi védelemre méltó jellege vagy a vagyontárgy funkcionalitása kap kiemelkedő büntetőjogi védelmet pl. az a lakosság ellátása, az ország gazdasági működése szempontjából igen fontos. Ezek a minősítés objektív szempontjai. Ezek mellett a magatartás szubjektív irányultsága is befolyásolhatja e cselekmények minősítését.

6. 6. 1. Erőszakos támadás a hardver- és az adathordozók ellen

Az informatika tudománya hardvernek nevezi a fizikailag létező egységek, eszközök, amelyek együttesen alkotják a számítástechnikai rendszert pl. billentyűzet (klaviatúra), mágneslemezek, nyomtatott áramkörök (chipek), képernyő (monitor), nyomtató (printer), egér, képolvasó (scanner) stb.

A technika fejlődése során és az adatfeldolgozás jellegére tekintettel is többféle adathordozófajtát használnak, így korábban lyukkártyát, lyukszalagot, mágnesszalagot, ma inkább hajlékony (floppy-) vagy kompakt lemezt (CD). Az a feltevés, hogy a munkahelyek elvesztését, munkakörök felszámolását jelentő számítógépesítés ellen a múlt század elejéről ismert luddita mozgalom "reinkarnálódik" és gyakoriak géprombolások lesznek szerencsére megalapozatlannak bizonyul. Napjaink Ned Ludd-jai kifinomultabb módszereket (pl. vírusprogramokat) alkalmaznak. Akcióikkal az adatállományt, illetve a számítógépes szoftvereket célozzák.

A fizikai léttel bíró dolgokban, tehát a technikai eszközökben és az adathordozókban véghezvitt erőszakos támadás tipikusan rongálás formájában mutatkozik meg.

A *rongálás* - az általános ismeretek szerint - olyan közvetlen vagy közvetett fizikai, kémiai esetleg ezek kombinációja révén megvalósuló ráhatás, amelynek eredményeképpen általában a vagyontárgyban állagkárosodás keletkezik.

A bűncselekmény tárgyi oldalán szereplő rongálás maga is gyűjtőfogalom. Többféle erőszakos magatartást foglal magában.

A *használhatatlanná tevés* azt jelenti, hogy a hardver vagy az adathordozó rendeltetésszerű használata - állagának károsítása nélkül - időlegesen vagy véglegesen kizárt. Sajátossága az, hogy az okozott sérelem általában helyrehozható pl. egy egyszerű példával élve, a kettétépett mágnesszalag összeragasztható.

Továbbá valamely elektronikus adatfeldolgozó- vagy adatátviteli rendszer használhatatlanná tehető a rendszer működését vezérlő számítógépes szoftver eltávolításával (törlésével) is.

Mivel a számítógépek és a számítástechnikai rendszert alkotó technikai eszközök ún. "összetett dolgok" (corpus ex cohaerentibus), így a használhatatlanná tétel formája a dolog szétszerelése, alkatrészeinek eltávolítása általában állagkárosodást nem eredményez.

A *megrongálás* esetén nem szükséges az, hogy ezen dolgok akár időlegesen is használhatatlanná váljanak, netán megsemmisüljenek. Rongálás esetében olyan károsodásról van szó, amely nem érinti, legfeljebb korlátozza a hardver vagy az adathordozó használhatóságát. Jellemzője a dologban beállott értékcsökkenés. Ilyenek pl. a technikai eszközre mért ütések vagy a mágnesszalag összegyűrése.

Viszont a legdurvább magatartás, a *megsemmisítés* következtében ezen eszközök eredeti állapota nem állítható helyre, ilyen magatartás lehet a technikai eszközök szétverése, felgyújtása, felrobbantása stb., továbbá az adathordozók szétszakítása, elégetése, szétmaratása savval stb. Technika - történeti kuriózumként említhetem, hogy a lyukkártyán és a lyukszalagon levő, a végrehajtani kívánt programnak megfelelő "feliratozás" (ún. statikus kódokkal való ellátás) mellé más,

hamis kódok felvitelével az adathordozó elveszti alkalmasságát az adott feladat elvégzésére, így ezt az adathordozó megsemmisítéseként kell értékelnünk.

A rongálás általában aktív magatartással valósítható meg. Ritkán a passzív tevékenység is értékelhető. Ez utóbbi esetben az a személy tartozik büntetőjogi felelősséggel, aki valamely jogszerű magatartás révén vagy munkahelyi kötelezettsége folytán megóvni köteles a dolgot, a technikai eszközöket, de ezt elmulasztja.

A bűnösség vizsgálata körében megállapítható az, hogy a bűncselekmény elkövetéséhez károkozási célzat (intentio nocendi) nem szükséges.

Az okozott kár tekintetében az egyenes szándék (dolus directus) mellett az eshetőleges szándék (dolus eventualis) is megalapozza a büntetőjogi felelősséget.

Az adathordozó ellen elkövetett erőszakos támadás az adatokban vagy programokban okoz károsodást. A kár értéke nem az adathordozó minimális értékéhez igazodik. Az adatok vagy programok "értékéről" később kissé tüzetesebben.

A hardver *fizikai létét* veszélyeztető erőszakos támadás büntetőjogi értékelésére a nemzetközi joggyakorlat kínálta alternatíva az alábbi:

1. Mivel az **osztrák**, a **finn**, a **svájci** büntető törvénykönyvekben "csupán" az adatok elleni megvalósuló támadást kriminalizálták, ebből az következik, hogy a hardver megrongálásának minősítése "megmarad" a hagyományos dologrongálás keretei között.[184]

2. Az **olasz** jogalkotók eltérő szabályozási módot választanak azzal, hogy a hardver nevesítésével speciális tényállással egészítik ki a Codice Penalet. Ebben a szakaszban nemcsak a hardver, hanem az adat vagy program megrongálása is helyet kap:

---

[184] Revue ... p. 151. 279. és 597.

"635. § (1) Aki részben vagy egészben megsemmisíti, megrongálja vagy használhatatlanná teszi más informatikai vagy teleinformatikai rendszerét ....
ha súlyosabb bűncselekmény nem valósul meg 6 hónaptól 3 évig terjedő szabadságvesztéssel büntetendő.
(2) A büntetés egy évtől 4 évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott tényállási elemek többször forognak fenn, vagy az elkövető a bűncselekményt rendszeroperátori minőségben követte el." [185]

Az első fordulat tevékenységi tárgyai folytán ezen tényállás speciális a hagyományos vagyonrongáláshoz képest. Az olasz törvény expressis verbis megnevezi ezeket a tárgyakat.

A tényállás egyben szubszidiárius is, mert akkor alkalmazható, ha a "közhasznú létesítmény elleni támadás" (Codice Penale 420. §) nem jön szóba.

A deliktum minősített esete az, ha a hardverben és az adatok vagy programokban történő károkozás megvalósul, valamint ha azt elkövető rendszeroperátori minőségét felhasználva valósítja meg a cselekményt. Ez utóbbi tehát delicta propria alakzat.

Hazánkban a Btk. 324. §-ban meghatározott rongálás tényállása a hardverek elleni erőszakos támadás büntetőjogi értékelésére megfelelő.

6. 6. 2. Intellektuális támadás az adatok- és a programok ellen

A hardver- és az adathordozó elleni erőszakos támadás során az adatok és a programok is - másodlagosan - sérelmet szenvedhetnek. Ugyanakkor az adatok és a programok "megrongálása" nemcsak fizikai hordozójuk tönkretételével történhet, hanem az előbbiek megváltoztatásával is. E cselekmények sajátossága az, hogy az nem dolog elleni erőszakban nyilvánul meg, hanem a számítógépes csalásnál illetve hamisításnál megismert intellektuális módon az adatok és programok manipulációjával.

A bűncselekmények tevékenységi tárgyai a számítógépes adatok, amelyek immateriális (láthatatlan, ki nem tapintható) javak.

---

[185] Leggi, decreti e ordinanze presidenziali ... id. közlöny 7.l. - saját fordítás

Az **ET. (89) 9. sz. Ajánlása** e körben háromféle cselekménytípust javasol kriminalizálni.[186]

I. Az adatok és a programok szándékos megváltoztatása.

II. Az adatokban és a programokban történő károkozás, amely az adatok vagy programok jogtalan törlésével, rongálásával, károsításával és elrejtésével érhető el.

III. A számítógépes szabotázs, azaz adatok és programok bevitele, törlése, elrejtése vagy bármely más módon megvalósuló befolyásolás, amelynek célja az elektronikus adatfeldolgozás- és adatátvitel akadályozása.

Ad I. Az adatok és programok szándékos megváltoztatása "csupán" az ET. (89) 9. sz. Ajánlásában a fakultatív listáján kap helyet. A jogosulatlan adatváltoztatás nem minden esetben jár együtt kár bekövetkeztével, hiszen lehetséges az, hogy ebből a cselekményből az érintett természetes vagy jogi személynek hátránya nem származik. Sőt, elméletileg az sem zárható ki, hogy ennek a jogellenes manipulációnak köszönhetően a pl. a program használhatóbb, "okosabb" lesz (pl. gyorsabban elérhető lesz egy-egy file, könyvtár).

Az adat és programváltoztatás módszerei ugyanazok, amelyeket a számítógépes csalásnál már láthattunk. Az adat- és a programváltoztatást csak abban az esetben javasolja szankcionálni az ET. ajánlása, ha az elkövetőt *szándékosság* terheli. Ugyanis ez a változtatás bekövetkezhet gondatlanságból is, pl. az adathordozón tárolt adatokat új adatokkal ír felül, jóllehet a korábbi adatokra lenne szükség vagy átengedi a számítógépét hiányosabb felkészültségű személynek, aki tudatlansága révén "könnyedén" beletörölhet valamely file-ba, ekkor az adatállományért felelős személyt legalább munkajogi felelősség terheli azért, mert a számítógép átengedésénél nem járt el kellő körültekintéssel. A gondatlan elkövetés az ET. ajánlásában nem szerepel.

A jogosulatlan adatváltoztatás azon esetére, amely károkozás hiányában is büntetőjogi felelősségre vonást eredményez az 1988-ban módosított **német** Btk.-ban

---

[186] CE Recommendation (89) 9. ..... p(s). 43-49.

található példa. A bűncselekmény önálló tényállásban a következő szövegezéssel szerepel:

"303/A. § (1) Aki adatokat jogellenesen töröl, eltüntet, használhatatlanná tesz vagy megváltoztat, két évig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő. (2) A kísérlet is büntetendő."

A tényállás elemzéséhez a német Btk. Kommentárját hívjuk segítségül.

Az adatváltoztatás a vagyon elleni deliktumok között, a vagyonrongálást (303. §) követően szerepel. A bűncselekmény tevékenységi tárgya az elektronikus adat. A deliktum akár egyenes, akár eshetőleges szándékkal is megvalósítható.

Míg az elkövetési magatartások jellemzése nem okoz problémát, addig a (2) bekezdés kísérlet értékelése nehézkes. A számítástechnikai rendszerhez telekommunikációs úton, azaz „kívülről" történő hozzáférés esetében a kísérlet megállapítása aggálymentes. A probléma az adatok közvetlenül klaviatúrán való bebillentyűzésénél merül fel. Vitatott lehet annak a tevékenységnek a minősítése, amikor az elkövető az adott file-ban dolgozva, lenyomja a klaviatúrán a billentyűt. Vajon befejezetté válik-e a bűncselekmény, vagy ez még csak annak kísérleti fázisa. A bűncselekmény a befejezettség stádiumába akkor jut, ha az adatváltoztatást az elkövető rögzíti is, vagyis lementi a számítógép memóriájába, illetve az adathordozóra. Hiszen amíg az adatokat nem rögzítik, addig azokat nem a számítógép nem változtatja meg, így eredeti formájukban maradnak meg. A bebillentyűzés tehát az adatváltoztatásra tett kísérletként értékelhető.

A bűncselekmény magatartás - tényállás. Nem szükséges, hogy a jogosulatlan adatváltoztatás kárt is eredményezzen.

Amennyiben az elkövető tevékenységével az elektronikus adatfeldolgozást akadályozza, úgy magatartása a német Btk.-ban 303/b. §-ában meghatározott komputer-szabotázsként értékelendő.[187]

---

[187] vö. Dr. Dreher - Dr. Tröndle ... s(n) 1709-1711.

Ad II. A számítástechnikában élenjáró országokban szerzett tapasztalatok azt mutatják, hogy az adat vagy a program megváltoztatásának a szándéka vagyoni kár előidézése.

Jellemzően a bosszúvágy által motivált cselekményekre hívják fel a figyelmet a szakirodalomban. Ezt annak a texasi férfinak az esetével illusztráljuk, aki a nyolcvanas évek végén elbocsátása előtt 150 ezer rekordot törlő vírust helyezett el a számítógépben.[188]

A vagyoni kárt eredményező *jogosulatlan adatváltoztatást* egyes országok eltérő módon kriminalizálják:

a. önálló tényállásban határozzák meg,

b. a vagyonrongálás tényállásának fordulataként vagy

c. a hardver rongálását büntető tényállásának részeként szabályozzák, és végül

d. nem alkotnak új tényállást, hanem a rongálás bűncselekményét alkalmazzák ezekben az esetekben is.

a. Az **osztrák** Btk. önálló tényállásban rendeli büntetni a jogellenes adatváltoztatást, ha az kárt okoz:

"126. § (1) Aki más személynek azzal okoz kárt, hogy az elektronikus úton feldolgozott, átvitt vagy átmenő adatokat, amelyekről nem vagy nem egyedül rendelkezhet megváltoztatja, törli, más módon használhatatlanná teszi, avagy megsemmisíti 6 hónapig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő.

(2) Az (1) bekezdésben meghatározott adat fogalmába nemcsak a személyekre, hanem egyéb adatok továbbá a programok is értendők.

(3) A büntetés 2 évig terjedő szabadságvesztés vagy 360 napi pénzbüntetés, ha az okozott kár a 25.000.- schillinget és 6 hónaptól 5 évig terjedő szabadságvesztés, ha az okozott kár az 500.000.- schillinget meghaladja." [189]

---

[188] adja hírül a Computerworld - Számítástechnika 1989/1. 7.lapon

[189] Strafgesetzbuch 10., durchgesehene Auflage. Wien (Manz * Taschenausgaben) 1990. s(n). 124-125. - saját fordítás.

b. A **finn** Btk. módosításakor a vagyonrongálás tényállását egészítik ki egy másik fordulattal:

"Aki abból a célból, hogy másnak kárt okozzon jogellenesen megsemmisít, töröl, elrejt vagy elhallgat számítógéppel vagy egyéb módon rögzített adatokat rongálást követ el és 4 hónaptól 4 évig terjedő szabadságvesztéssel büntetendő." (35. fejezet 1. §)[190]

A **svájci** büntető törvénykönyvben szintén a vagyonrongálás tényállásához fűzik az adatok megrongálását:

"144. § (2) Büntetendő az is, aki az elektronikusan vagy más módon tárolt vagy átvitt adatot törli, megváltoztatja vagy teszi használhatatlanná.

(3) Hatályon kívül helyezve.

(4) A büntetés fogházban letöltendő öt évig terjedő szabadságvesztés, ha a cselekmény nagy értékű kárt okoz.

A bűncselekmény hivatalból üldözendő." [191]

c. Az **olasz** Btk.-ban a hardver megrongálásának második fordulatában szerepel az adatokban történő károkozás: "

635. § (1) Aki részben vagy egészben megsemmisíti, megrongálja vagy használhatatlanná teszi .... más adatait vagy programjait, ha súlyosabb bűncselekmény nem valósul meg 6 hónaptól 3 évig terjedő szabadságvesztéssel büntetendő."[192]

Emlékeztetőül a minősített eset a hardver és az adat vagy programban történő károkozás egyidejű, továbbá ha az elkövető rendszeroperátor.

---

[190] Centenary of the Finnish Penal Code ... id. kiadvány p. 14. - saját fordítás.

[191] www.gesetze.ch/sr/311.0/311.0_012.htm

[192] Leggi, decreti e ordinanze presidenziali ... id. közlöny 7. L. - saját fordítás.

d. Mivel **Japánban** a szoftvert és az adathordozón rögzített adatokat vagyontárgynak tekintik, így ezek megrongálása egyszersmind a Btk. 261. §-ban írt vagyonrongálásnak minősül.[193]

Az elektronikus adatfeldolgozás növekvő társadalmi - gazdasági jelentőségére tekintettel a számítógépben vagy valamilyen adathordozón tárolt adatok védelmének fokozása érdekében **hazánkban** de lege ferenda szükségesnek tűnik a jogellenes adatváltoztatás kriminalizálása abban az esetben, ha az kárt okoz az elektronikus adatfeldolgozó rendszer üzemeltetőjének, tulajdonosának vagy annak, akinek az érdekében folyik ez a tevékenység.

Ez a tényállás az informatikai bűncselekmények második generációját jelentené a magyar büntetőjogban.

A jogosulatlan adatváltoztatás elkövetőjével szemben alkalmazandó, alkalmazható büntetőjogi szankciók természetesen nem helyettesítik, nem helyettesíthetik a polgárjogi kárigény érvényesítését akár a munkavállalóval, akár kívülálló személlyel szemben. Az előbbi körben a munkajogi felelősség sem kizárt, ha a munkáltató emellett dönt.

A jogellenes adatváltoztatást a vagyon elleni bűncselekmények között, akár önálló tényállásban, akár a rongálás tényállásába illesztve célszerű ma még megfogalmazni. De lege ferenda megoldásként továbbgondolásra javaslom az alábbi szövegezést:

"Aki program vagy adat megváltoztatásával, törlésével, téves vagy hiányos adat betáplálásával, illetve egyéb, meg nem engedett műveletek végzésével az elektronikus feldolgozásra rendelt adatokban kárt okoz, ha más bűncselekmény nem valósul meg vétséget követ el és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő."

A bűncselekmény tevékenységi tárgya olyan számítógépes adat, amely akár a számítógép memóriájában, akár adathordozón rögzített.

A tárgyi oldalon levő elkövetési magatartások ugyanazok, amelyek a számítógépes csalás definíciójában már szerepelnek. Tehát e körbe tartozik a program megváltoztatása, adatok törlése, téves vagy hiányos adatok betáplálása, továbbá bármilyen más tevékenység - és itt válna nyitottá a tényállás - amely alkalmas arra, hogy az elektronikus adatfeldolgozás eredményét befolyásolja.

A bűnösség kapcsán megállapítható, hogy a bűncselekmény megvalósulásához rongálásra irányuló célzat (intentio nocendi) nem szükséges, ugyanakkor a bűncselekmény csak szándékosan valósítható meg. Az elkövető tudatában van azzal, hogy cselekménye jogellenes, amelynek corollariumaként kár fog bekövetkezni, és ez utóbbit kívánja vagy abba belenyugszik.

Csak emlékeztetőül számítógépes csalás esetében az elkövető saját vagy harmadik személy számára jogtalan vagyoni haszonszerzés végett cselekszik.

A rongálásra indítéka (causa motiva) közömbös. Még a harmincas években a német **Sauer** a rongálás elkövetői típusai között megkülönböztetett:

1. a tiszta károkozó típusú elkövető pusztán rongálás szándékával cselekszik,
2. a károkozási szándék mellett más motívum is vezérelheti az elkövetőket:

- a meggyőződéses típusú elkövető érdekei védelmében, elégtételt véve cselekszik,
- a haszonszerzésre irányuló típusú elkövető más vagyonának megrongálásból hasznot remél.[194] Ez utóbbi elkövetői - típus gyakorisága napjaink kiélezett piaci versenyében realitás.

A deliktum az ún. számítógépes vírusprogramok alkalmazóival szemben is felhívható. A tényállás szubszidiárius lenne, csak akkor kerülhet megállapításra, ha más bűncselekmény nem valósul meg. Ugyanakkor el kell határolnunk a következő pontban tárgyalandó szabotázs - jellegű cselekményektől is:

---

[193] Revue ... p. 443.

[194] idézi: Angyal Pál: A vagyonrongálás és gyújtogatás (A magyar büntetőjog kézikönyve 12. kötet) Bp. 1935. 18.l.

- A közveszélyokozás (Btk. 259. §) esetében az elektronikus adatfeldolgozásba történő beavatkozás, a jogosulatlan adatváltoztatás a sugárzó vagy más anyag, energia pusztító hatásának kiváltását eredményezi.
- A közérdekű üzem működésének megzavarása (Btk. 260. §) megvalósul abban az esetben, amikor az elkövető valamely közérdekű üzem elektronikus adatfeldolgozó- és átviteli rendszerébe avatkozik be, és ez eredményezi a működésbeli zavarokat.

Ad III. Ma már számítógépes rendszerek vezérelnek egy - egy ipari, mezőgazdasági, energiatermelő- vagy szolgáltató, postai - vagy honvédelmi-, távközlési-, bánya-, és egyéb a lakosság, illetve a nemzetgazdaság szempontjából rendkívül fontos üzem működését. Az ilyen üzemek büntetőjogi védelme természetesen relatív állandósággal jelen vannak a büntetőtörvénykönyvekben. Elegendő utalnom az 1810. évi francia Code Penal III. fejezetére, amely a gyújtogatás, robbantás, vízáradás előidézését pönalizálja.[195]

Az közérdekű üzemek számítógépes rendszerei ellen véghezvitt akár erőszakos, akár intellektuális támadások azonban a természetes személyek széles körét is érinthetik, veszélyeztethetik, valamint potenciálisan óriási anyagi károkat, pusztításokat okozhatnak.

Az ET. (89) 9. sz. Ajánlás szerint számítógépes szabotázs az adatok és programok bevitele, törlése vagy elrejtése vagy a számítógépes rendszerek más módon történő befolyásolása azzal a szándékkal, hogy a telekommunikációs rendszerek, mint számítógépes rendszerek funkcionálását akadályozzák.

A definíció mellőzi a hardver elleni támadást és csupán az adatok és/vagy programok elleni támadásra koncentrál. Viszont az elektronikus adatfeldolgozó- és átviteli rendszerek működése, rendeltetése elleni támadás lehetőségeibe beletartozik a hardver elleni támadás is.

---

[195] Angyal Pál: A vagyonrongálás ... id. mű 10.l.

Ehelyütt csupán azon országok törvényhozási eredményeit emeljük ki, ahol az elektronikus adatfeldolgozási- és átviteli rendszerek ellen végrehajtott támadást nevesítik ezekben a tényállásokban.

A **német** Btk.-ban 1988-tól szankcionálják a számítógépes szabotázst.

"303/B. § A komputer - szabotázs

(1) Aki egy idegen üzem, vállalkozás vagy hatóság számára lényeges jelentőségű adatfeldolgozást azáltal zavar meg, hogy

1. a 303/A. § (1) bekezdésben írt cselekményt követ el, vagy

2. az adatfeldolgozó berendezést, illetve adathordozót megkárosítja, megsemmisíti, használhatatlanná teszi, eltávolítja, valamint megváltoztatja pénzbüntetéssel vagy öt évig terjedő szabadságvesztéssel büntetendő.

(2) A kísérlet is büntetendő."

Mivel ez a tényállás is új típusú bűncselekmény ismérveit tartalmazza, ezért kissé részletesebben tekintjük át, a már citált kommentár ismételt felhívásával.

A bűncselekmény jogi tárgya kettős. Egyfelől az adatfeldolgozás folyamatának zavartalansága, másfelől a számítástechnikai eszközök biztonsága.

A bűncselekmény tevékenységi tárgyai az elektronikus adatfeldolgozásra szolgáló berendezések és az adathordozók. Az előbbi körből kiesnek a mikrochipeket tartalmazó elektronikus írógép vagy számológép. Ugyanakkor valamennyi adathordozófajta idetartozik.

Az elektronikus adatfeldolgozás akadályozása részben a rongálás gyűjtőfogalmába tartozó magatartások révén, továbbá más magatartásokkal, így az adatfeldolgozó berendezés vagy adathordozó eltávolításával, mint a lopás résztevékenységével, illetve az adathordozó megváltoztatásával valósul meg. Részben az adatmanipuláció körébe sorolandó - és fentebb már részletezett - magatartásokkal valósítható meg. (Az ET. ajánlásában a programmanipuláció nem szerepel.)

A sértetti kör tágnak tekinthető. A német Btk. kommentárja kiemeli, hogy ipari, gyári és mezőgazdasági üzemek mellett kutatóintézetek, kórházak, gyógyszertárak, orvosok, ügyvédek, vásárigazgatóság, sőt színház elektronikus adatfeldolgozó rendszere ellen is elkövethető a bűncselekmény.

A Kommentár szerint az adatfeldolgozó tevékenység ellen végrehajtott szabotázs akkor büntetendő, ha az a sértett számára lényeges jelentőséggel bír. E kérdés eldöntésében nem az adatfeldolgozás terjedelme a döntő, hanem a vállalkozásnál betöltött szerepe vizsgálandó.

A szabotázs az elektronikus adatfeldolgozó- és átviteli tevékenységet közvetlenül kell, hogy érintse.[196]

A **holland** Btk. rendkívül részletes szabályai magukba foglalják a mi fogalmaink szerinti közérdekű üzem működésének megzavarásának, illetve a közveszélyokozásnak elemeit is:

"161f. § Aki szándékosan megrongál, megsemmisít vagy használhatatlanná tesz bármely automata rendszert, amely adatok tárolására, feldolgozására szolgál, illetve bármely adatátviteli rendszert, vagy ennek telepítését, működését használhatatlanná teszi, megzavarja továbbá hatástalanít bármely olyan biztonsági intézkedést, amelyet a rendszernél alkalmaznak,

1. a büntetés hat hónapig tartó szabadságvesztés vagy 100.000.- guldenig terjedő pénzbüntetés, ha ez a bűncselekmény megakadályozza vagy meggátolja a közhasznú adattárolást vagy feldolgozást, továbbá a telekommunikációs hálózat megrongálását eredményezi;

2. a büntetés hat évig terjedő szabadságvesztés vagy 100.000.- guldenig terjedő pénzbüntetés, ha ez a bűncselekmény súlyos veszélyt jelent a közszolgálat ellátására, termékeire;

3. a büntetés kilenc évig terjedő szabadságvesztés vagy 100.000.- guldenig terjedő pénzbüntetés, ha a bűncselekmény mások életét veszélyezteti;

---

[196] vö. Dr. Dreher - Dr. Tröndle ... s. 1711-1713. és vö. Dr. Harro Otto ... s. 123-131.

4. a büntetés tizenöt évig terjedő szabadságvesztés vagy 100.000.- guldenig terjedő szabadságvesztés, ha ez a bűncselekmény mások életét veszélyezteti és halált okoz.

350a. § (1) Aki automatizált rendszerben tárolt, létre hozott vagy továbbított adatot jogellenesen megváltoztat, töröl, használhatatlanná illetőleg hozzáférhetetlenné tesz vagy ezt kiegészíti két évig terjedő szabadságvesztéssel vagy 25.000.- guldenig terjedő pénzbüntetéssel büntetendő.

(2) Aki az első bekezdésben meghatározott cselekményt távközlési rendszeren keresztül történő jogosulatlan behatolás révén követi el, és ezzel kárt okoz négy évig terjedő szabadságvesztéssel vagy 25.000.- guldenig terjedő pénzbüntetéssel büntetendő.

(3) Aki jogellenesen elérhetővé tesz vagy terjeszt olyan adatot, amely arra szolgál, hogy önmagát megsokszorozva egy automatizált rendszerben kárt okozzon négy évig terjedő szabadságvesztéssel vagy 100.000.- guldenig terjedő pénzbüntetéssel büntetendő.

(4) Nem büntethető a (3) bekezdésben meghatározott bűncselekmény elkövetője akkor, ha cselekménye az ilyen adatok által okozott kár csökkentését célozza.

351.§ Aki szándékosan megrongál, megsemmisít vagy használhatatlanná tesz vasúti vagy olyan elektronikus adatok tárolására vagy feldolgozására szolgáló automata-rendszert, továbbá olyan távközlési rendszert, árvízvédelmi-, vízkibocsátó- gáz-, vízellátó-, illetve szennyvízüzemet, amelyek közhasznúak vagy a nemzetvédelem szempontjából fontosak három évig terjedő szabadságvesztéssel, vagy 25.000.- gulden pénzbüntetéssel büntetendő." [197]

A holland szakirodalomban a 161f. §-161g. § szakaszok, a fizikai szabotázst, a 350a.-350b. §, az ún. logikai szabotázst szankcionálják.

---

[197] www.minjust.nl:8080/C__ACTUAL/PERSBER/compcrim.htm - saját fordítás.

Az első két tényállás megnevezi a tevékenységi tárgyakat. Ezek az elektronikus adatfeldolgozásra, adattovábbításra, adatátvitelre szolgáló berendezések.

Az elkövetési magatartások között viszont nemcsak a rongálás szerepel, hanem a biztonsági intézkedések hatástalanítása is.

A következő 161g. §, amelyet terjedelmi okokból nem idézek delictum sui generis bűnsegédi alakzatot rendeli büntetni.

A bűnsegéd felelőssége hasonlóan tagolódik, mint a tettesé, csupán alacsonyabb büntetési tételekkel. (A pénzbüntetés maximuma 25.000.- gulden, a szabadságvesztés büntetés mértéke az esetekhez igazodva három hónaptól egy évig terjed.)

A 350a. - 350b. §-okban meghatározott bűncselekmény elkövetési tárgyai nemcsak a számítógépes rendszerben *tárolt* adatok, hanem ezen rendszereken át *áramló* adatok is.

A 350a. § szolgál az adathordozó elleni erőszakos támadás értékelésére akkor, ha annak következtében az adatok megrongálódnak.

Minősített esetben szerepel a hacking útján, azaz az "elektronikus betöréssel" végrehajtott adatmódosítás is, feltéve ha a számítógépes rendszerbe történő jogosulatlan belépés kárt okoz.

Külön érdekessége ennek a tényállásnak, hogy a vírusprogrammal megvalósított adatok elleni támadás először szerepel nevesítve a minősített esetben.

A 350b. § pedig a bűnsegéd büntetni rendeltségéről szól. (A holland Btk. a bűnsegélyi magatartás büntetési tételét minden esetben egy hónapban maximalizálta 10.000.- gulden pénzbüntetéssel alternativításban.)

A 351. § pedig azt az esetet szankcionálja, amikor az elektronikus adatfeldolgozó- és átviteli rendszerek elleni akár fizikai, akár ún. logikai szabotázs közveszélyt idéz elő.

A **finn** Btk. 1990-es módosításakor szabotázs bűncselekményeként szabályozza az alábbiakat:

"Aki cselekményével

1. tűzvészt,

2. robbanást,

3. árvizet vagy

4. természeti katasztrófát idéz elő és ezzel általánosan veszélyezteti az életet és egészséget, vagy másnak jelentős anyagi kárt okoz szabotázs bűncselekményét követi el és négy hónaptól négy évig terjedő szabadságvesztéssel büntetendő.

Aki vagyontárgy megrongálásával vagy megsemmisítésével, továbbá termelő-, elosztó-, információs hálózat működési rendszerébe történő jogellenes beavatkozással komoly károkat az energiaellátás, közegészségügy, nemzetvédelem, igazgatás vagy más a társadalom számára fontos funkció ellátása terén szintén elköveti a szabotázs bűncselekményét.

A kísérlet is büntetendő." [198]

1993-tól az **olasz** Btk.-ban szintén a közhasznú létesítmények elleni támadás tradicionális tényállása egészül ki:

"420. §: Aki közhasznú létesítményt megrongálására vagy megsemmisítésére törekszik, amennyiben súlyosabb bűncselekmény nem valósul meg, egy évtől négy évig terjedő szabadságvesztéssel büntetendő.

Az első bekezdés szerint büntetendő az, aki közhasznú informatikai illetve teleinformatikai rendszerek vagy ezekben feldolgozott, tárolt adatok, programok megrongálására vagy megsemmisítésére törekszik.

A büntetés három évtől nyolc évig terjedő szabadságvesztés, ha ezen létesítményeket, rendszereket, adatokat, programokat megrongál vagy megsemmisít vagy e létesítmény, rendszer működésének részleges megszakítását eredményezi."[199]

---

[198] Centenary of the Finnish Penal Code ... id. kiadvány p. 37. - saját fordítás

[199] Leggi, decreti e ordinanze presidenziali ... id. közlöny 5. l. - saját fordítás

Ez a szakasz a közhasznú adatfeldolgozó- és átviteli rendszerek megrongálásának illetve megsemmisítésének előkészületét és befejezett bűncselekményi alakzatát egyaránt szabályozza.

Az olasz törvényhozás ezzel kívánja kifejezésre juttatni a büntetőjogi védelem fontosságát, szigorát.

A holland, a finn és az olasz törvényhozási példák *közös vonása* az, hogy mind a közveszélyokozás, mind a közhasznú (közérdekű) üzem működésének megzavarását szankcionáló törvényi tényállását egészítik ki az elektronikus adatfeldolgozó- és átviteli rendszerek nevesítésével.

A **magyar** Btk. Különös részében a XVI. fejezet I. címében meghatározott közbiztonság elleni bűncselekmények közé felvett közveszélyokozás és a közérdekű üzem működésének megzavarása deliktumai elegendőek az elektronikus adatfeldolgozó- és átviteli rendszerek elleni szabotázs cselekmények minősítésére.

Mivel mindkét törvényi tényállásban az elkövetési magatartások exemplifikatív felsorolását találjuk, így az adatok és/vagy programok manipulálása, mint az ún. logikai szabotázs, és az erőszakos fizikai támadás értékelésének nincs akadálya.

Véleményem szerint a fentebb már említett jogellenes adatváltoztatás kriminalizálásán túl a büntetőjog által védett tárgyak törvényi megjelenítésének fontossága miatt szükségesnek tűnik az *elektronikus adatfeldolgozó- és átviteli rendszerek* expressis verbis megnevezése a Btk. 259. § (1) bekezdésében, valamint a Btk. 260. § (4) bekezdésében.

A számítógépes adatok és programok elleni intellektuális támadás egyik speciális, viszont rendkívül veszélyes és alattomos formája **a számítógépes vírusok** alkalmazása.

A hetvenes években csupán szakmai körökben "suttognak" róla, de a nyolcvanas években már a szélesebb szakmai körökben tért hódít egy új fogalom, a

vírusprogram. A fogalom eredete az orvostudomány hasonló kategóriájából származik. Ugyanis a komputervírus szintén egy gócpontból kiindulva "fertőzi meg" az adatállományokat, programokat. A sajtóban e vírusokról pusztító hatásuk miatt "számítógépes AIDS-nek" valamint "delírium digitalis-nak" vagy hasonló hangzatos elnevezésekkel találkozunk.[200]

A vírusok *hatásukat* tekintve sokfélék. Nézzünk néhány ismertebb vírust. Vannak ártatlan, "tréfáskedvű" vírus. Bár igen bosszantó, ha a Yankee Doodle-t az Oscar - díjas James Cagney helyett a számítógép dúdolja. A "dalolóvírusok", mint pl. az "Ötórai tea" egyike már bemutatkozott a Magyar Nemzeti Bank számítógépeiben 1992-ben.[201] Rendkívül rossz tréfa a "Potyogós" - (vagy Cascade) vírus, amelynek hatása abban áll, hogy általa a képernyőre kiírt betűk "leesnek". E vírusoknál komolyabbak a Péntek 13. vagy az Exeburg vírusok. Az előbbi, amelyet palesztin diákok alkotnak, és szovjetek tökéletesítenek, akkor pusztít a számítógépben, ha a pénteki nap a hónap 13. napjára esik, míg a másik minden olyan szókapcsolatot töröl, amelyben megtalálható "március" szó.[202]

Ugyanígy "időzített bomba-vírusként" március 6-án lép működésbe az egy tipikus boot-vírus a Michelangeló - vírus, vagy az augusztus 5-én feltűnő Androméda - vírus. Ma már majdnem mindennapra várható valamilyen vírus, mint hívatlan vendég.

A vírusok legveszélyesebb típusai igen komoly károkat is képesek előidézni.
- 1985. márciusában a los angeles-i Víz- és Energiaügyi Részleg számítógépeit a vírusok egyik fajtája, egy "logikai bomba" bénítja meg.[203]
- 1988-ban egy Robert Morrison Cornell nevezetű, akkor 24. éves egyetemi hallgató 6000 /!/ számítógépet fertőz meg, köztük a féltve óvott NASA, US. Air Force legvédettebb rendszereit. [204]

---

[200] vö. Dr. Harro Otto ... s. 129 -130.

[201] adja hírül a Népszabadság 1992. február 29. 4. lapon
[202] Kiss János - Szegedi Imre: Új víruslélektan. Budapest, 1991. 15.1
[203] adja hírül a Heti Világgazdaság 1992. február 29-i számában a 39-40. lapon
[204] adja hírül a Magyar Nemzet 1990. június 9. 9. lapon

- 1992. június 24-én két párizsi repülőtér forgalma áll le 90 percre, mert egy vírus került a központi komputerbe.[205]

Ismertek katonai célú vírusok is, amelyek a szembenálló fél védelmi rendszerének számítógépeit blokkolják. Egyelőre nem lebbentik fel a fátylat arról a titokról, hogy az amerikaiak légi fölénye az Öböl-háborúban az iraki légvédelmi rendszert bénító vírusoknak köszönhető-e vagy sem.[206]

A vírusok tipizálása a szakirodalomban különböző. Egyes szerzők a hatásuk szerint különböztetik a vírusokat, ennek alapján léteznek program- vagy adatállományt felülíró, és rendszervírusok, amelyek a merevlemezt és a hajlékony lemezt teszik használhatatlanná.[207]

A vírusok hatása éppúgy lehet átmeneti (pl. dallamlejátszás, az adatfeldolgozás lassítása továbbá ábrák, szövegek megjelenése a monitoron) vagy állandó (pl. file-ok tartalma megváltozik, megsemmisül).

Mivel a vírusprogramok zöme alkalmas arra, hogy az elektronikus adatfeldolgozás- és átvitel folyamatát hátrányosan érintse, befolyásolja vagy bénítsa - ha a készítője jelenleg nem is, de - az a személy, aki a vírust a számítógépbe juttatja a megfelelő tényállás felhívásával (pl. a német vagy holland számítógépes - szabotázs, finn szabotázs, a hazai közérdekű üzem működésének megzavarása (Btk. 260. §) vagy harckészültség veszélyeztetése (Btk. 363. §) stb. alapján) büntetőjogi felelősséggel tartozik.

6. 7. A számítógépes zsarolás

A számítógépek sokoldalúsága nemcsak a társadalmi - gazdasági szférában hasznosul, hanem a legkülönfélébb bűncselekmények elkövetési eszköze lehet

---

[205] adja hírül a Kurír 1992. június 25. 5. lapon
[206] adja hírül a 203. pontban említett Heti Világgazdaság
[207] Kiss János - Szegedi Imre id.mű .... 69-72.l.

egyben. Az a tény, hogy számítógépet erőszakos vagyon elleni deliktum megvalósítására szántak túlszárnyalja a kriminalisták képzeletét.

1992. február 2-án tartóztatják le Ohióban *Dr. Joseph Lewis Popp*-ot, akit a számítógépes vírus atyjának tartanak. Ez a tehetséges férfiú, aki elvégzi a Harvardot, majd több ENSZ - szervezetnél is, mint szakértő dolgozik, nem más talál ki, mint azt, hogyan lehet számítógéppel zsarolást elkövetni.[208] Egy programot ír, amely címében az AIDS-re vonatkozó információkat tartalmazta. Ez azonban valójában egy "trójai faló" program. Az "AIDS Information Disk" számítógépbe történő betöltése után arra szólítja fel a felhasználót, hogy küldjön pénzt a felhasználás jellegétől függően 189.- vagy 378.- amerikai dollárt egy privát panamai postafiók címére. Ennek fejében Popp küldeni fog egy újabb szoftvercsomagot. Ellenkező esetben a lemezen rögzített program 90. hozzáférést (újraindítást) követően tönkreteszi, pontosabban a felhasználó számítógépében rögzített adatállományát titkosítja. Az inkriminált lemezeket Popp angliai és panamai címekről 26.000 címzettnek küldte el, amelyekből Magyarországra is érkezett két (?) lemez.[209] Joseph Lewis Poppot *zsarolás* bűncselekményéért vonják felelősségre.

A cselekmény minősítéséhez - véleményem szerint - a **magyar** Btk. 323. §-ában zsarolást meghatározó rendelkezése is aggálymentesen alkalmazható. Hiszen az elkövető azzal fenyegeti meg a hajlékony lemez felhasználóját, hogy a program újraindításával használhatatlanná teszi az adatállományát, amennyiben nem kapja meg a programban feltüntetett pénzt (causalis nexus). Ha a felhasználó eleget tesz a követelésnek, úgy "megújíthatja a szoftverbérletet", vagyis kap egy másik programot, amellyel az előzőt negligálhatja. Feltéve, ha azon nem olvasható egy újabb követelés egy immár harmadik program rendelése céljából és így folytatódna a sor .... Más oldalról tehát az elkövető vagyoni haszonszerzés (animus lucri) céljából fenyegeti meg a hajlékony lemez használóját.

---

[208] "Törvény a számítógépes visszaélésről és részletek a törvényjavaslat parlamenti vitájából" (az Egyesült Királyságban) Informatika - Jog - Közigazgatás IV. kötet Bp. 1992. 24.11 lapon és Kis János - Szegedi Imre id. mű. 33 - 34.l.

[209] v.ö. 208. sz.

A zsarolás bűncselekménye a kár bekövetkeztével válik befejezett, amely ebben a konkrét esetben a program 90. újraindításával realizálódik. Ennek hiányában a bűncselekmény kísérleti stádiumban marad.

6. 8. Az adatkikémlelés

A számítástechnika fejlesztésének legfőbb ösztönzője a nagytömegű és a gyors adatkezelés igénye és szükségessége.

A szilíciumchipek méretcsökkentése és a számítógépek működési sebessége már közel került a fizikai megvalósíthatóság határához. Egy évtizede megkezdődtek kvantumelektronikai kutatások azzal a céllal, hogy további méret csökkentések következhessenek és ezzel a tároló- kapacitások bővítése váljon lehetővé.

Az elektronikus adatfeldolgozó- és átviteli rendszerek terjedésével, az adatok tartalmának sokszínűvé válásával az ilyen rendszerekben tárolt adatok jogosulatlan megszerzésére, megismerésére irányuló törekvések is felerősödtek.

A British Telecom 1994-ben több ezer hívószámot kénytelen volt megváltoztatni, mivel egy hacker behatolt abba az adatbankba, ahol az államtitkot képező telefonszámot tároltak.[210]

Az ipari - gazdasági és katonai kémkedés, a hírszerzői munka módszerei is mára megújultak, legalábbis kibővültek. Ennek a "második legősibb mesterségnek" a gyakorlásához már nemcsak a piciny "poloskák", és kamerák, a szállodai szobák átkutatása, a szexuális kapcsolat kierőszakolása, a "ösztöndíjasok" kiküldése, a vesztegetés, a zsarolás más módszerek tartoznak az eszköztárába, hanem a számítógépes környezetben megvalósított adatkikémlelés is. Nemzetközi tapasztalatok szólnak amellett, hogy az előtérbe került ipari - gazdasági hírszerzés, az ún. "versenyinformációk" (pénzügyi - gazdasági, technológiai, értékesítési információk, stratégiai tervek stb.) megszerzésére irányuló egyre gátlástalanabb törekvés.

---

[210] adja hírül az Új Dunántúli Napló 1994. december 28. 8. lapon

Az angolszász szakirodalomban elterjed a "bitnapping" kifejezés, amely egy szellemes szójáték a "kidnapping" (a gyermekrablás, tágabban értelmezve az emberrablás) analógiájára.

Az adatállományokat a legkülönfélébb módon igyekeznek védeni az illetéktelen "szemek" elől, kezdve a rendszer fizikai biztosításától, a számítógép használatának, valamint az adatállományok kódokkal történő védelmén át magának az adatok titkosításáig.

Az adatok kódolása következményeként a külvilág, azaz az illetéktelenek számára érthetetlen és értelmezhetetlen adathalmaz jelenik meg. Mivel nem létezik megfejthetetlen kód, ezért "csupán" arra lehet törekedni, hogy a kód feloldása több időt vagy anyagi ráfordítást igényeljen, mint amennyit az adat "ér". Ezzel együtt az adatok jogosulatlan megismerésének és megszerzésének, az adatlopások módjai is változatosak:

1. A rendszerbe történő jogszerű belépést vagy jogellenes behatolást követően az adatok a számítógép memóriájából vagy egyéb adathordozóról lehívhatók, megtekinthetők monitorón, átvihetők más adathordozóra vagy kinyomtathatók stb. Ebben az esetben k ö z v e t l e n ü l férkőzhet az adatokhoz.

2. Az adatok megismerhetők k ö z v e t e t t e n is, így pl. a mágneslemezek-, szalagok, lyukkártyák- és szalagok, a hajlékony, kompakt lemezek vagy akár a számítógép, az ebből kiszerelhető merevlemez eltulajdonításával is. A közvetett módszerek közé tartozik ma már a telefon- és adatátviteli vonalak "megcsapolása", valamint passzív módon megvalósítható a monitorok elektromágneses sugarainak "lehallgatása" is. A magyar MHB "társbérlőjével" levő Puma magyarországi leányvállalatával 1992-ben vitába keveredik, mert a bank biztonsági megfontolásokból, a számítógépek monitorai sugárzásának jogosulatlan "lehallgatását" megakadályozandó befalaztatott egy olyan bejárati ajtót, amelyet a Puma cég dolgozói használtak.[211]

---

[211] adja hírül a Népszabadság 1992. december 14. 4. lapon

Az adatkikémlelés fogalma tehát - véleményem szerint - felöleli az adatok jogellenes megismerését illetőleg, ha ezen adatok tárgyi eszközön (adathordozón vagy papírra nyomva stb.) jelennek meg, akkor adatok jogellenes megszerzését.
Ez a különbségtétel láthatóan viszonylagos, hiszen pl. az adatok képernyőn történő kiíratásával az adatok az elkövető ismeretébe kerülnek, tehát azokat "megszerezte". Az adatok jogtalan megszerzésének büntetőjogi szankcionálása a tradicionális titoksértő tényállások alapulvételével oldható meg.

A titok fogalmába tartoznak azok az ismeretek: amelyek
a. meghatározott személy(ek) tudatában léteznek,
b. az ismeretek ezen személy(ek) érdekét szolgálják vagy akaratát testesítik meg,
c. ebből következően az ilyen ismeretek megszerzése viszonylagosan korlátozott, vagyis csupán meghatározott személy(ek) férhet(nek) hozzá szabadon (ezek pozitív feltételek). Ugyanakkor mások nem vagy csak korlátozott formában ismerhetik meg (ez tehát negatív feltétel).[212]

A titokvédelmet biztosító tényállások a büntető törvénykönyvekben relatív állandósággal jelen vannak. Tekintettel arra, hogy a titok olyan sajátos eszmei érték, amely évszázadok óta, az átalakuló politikai - gazdasági rendszerek közepette is büntetőjogi védelemben részesül. Természetesen konkrét tartalma, a védendő titkok körének meghatározása tükrözte és tükrözi kora politikai - gazdasági viszonyait, érdekeit.

Az első jogi emlék a Kr.u. 506-ból származó Lex Romana Visigothorum, amely a végrendelet vagy más irat jogosulatlan felbontását bünteti.[213]
A jogfejlődés során a büntetőjog által védett *titkok tárgyai* mára az alábbiak:

---

[212] Dr. Angyal Pál: A titok védelme anyagi és alaki büntetőjogunkban. Budapest, 1908. 22 - 34. l.

[213] Dr. Angyal Pál: A titok védelme ... id. mű 36.l.

a. állam-,

b. szolgálati-,

c. üzleti-,

d. bank- és

e. magántitok.

A titkok többféleképpen kerülhetnek *ismeretünkbe:*

a. hivatali tevékenység útján (pl. közhivatalnok),

b. hivatás gyakorlása során (pl. ügyvéd, orvos)

c. bizalmi jogviszony alapján.

A titok *megjelenhet:*

a. tudatunkban, ekkor eszmei titokról beszélünk, avagy

b. tárgyi eszközön (iraton, levélben, mikrofilmen, hajlékony- vagy kompakt lemezen stb.), ezt tárgyi titoknak nevezhetjük.

A titok tárgyára tekintettel több tényállás is található a büntető törvénykönyvekben. Hazánkban az állami-, a szolgálati-, a hivatali-, magán-, üzleti-, és banktitok élvez büntetőjogi védelmet. Ha a számítógépes adatok titkot képeznek, úgy azok bármilyen - fentebb említett - módon történő megszerzése, felhasználása, jogosulatlan személy számára hozzáférhetővé vagy illetékes személy számára történő hozzáférhetetlenné tétele a tradicionális titoksértő tényállások révén már kriminalizált. E szerint a titok megszerzése olyan céltudatos tevékenységet jelöl, amely a titok megismerésére koncentrál. Ez akár a titokkal történő közvetlen érintkezéssel, akár a titok hordozójának birtokba vételével valósulhat meg.

A hozzáférhetővé tétel azt jelenti, hogy az elkövető olyan helyzetet teremt, amely által a titok tartalma valamely illetéktelen személy tudomására jut (pl. átadja).

A hozzáférhetetlenné tétel esetén az elkövető az ismeret közlését az illetékes személy felé időlegesen vagy véglegesen elmulasztja.

Nem minden adat képez azonban titkot. Számítógépes környezetben ennek fordítottja igaz, vagyis minden az elektronikus adatfeldolgozás-, és átvitel folyamatában szereplő titok adatként szerepel a számítógép memóriájában vagy bármely adathordozón. Ugyanakkor a jogosulatlan adatszerzés e tevékenységek védettségének megtörését, sőt ezáltal megzavarását is jelenti és emiatt több országban megteremtik e cselekmények büntetőjogi üldözésének feltételeit.

Az 1986-os **német** büntető törvénykönyv módosításával egy ún. "formális titoksértő" tényállás alkotásával büntetni rendelték az adatok kikémlelését.
"202/A.(1) Aki más részére szánt és illetéktelen hozzáférés ellen védett adatot jogosulatlanul magának vagy másnak megszerez három évig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő.
(2) Az első bekezdés értelmében csak az minősül adatnak, amit elektronikusan, mágneses vagy egyébként közvetlenül nem észlelhető módon rögzítettek."

Az adatok kikémlelés a levéltitok megsértésének tényállását követi, így látható, hogy ez cselekmény *quasi* titoksértés. Ha az elkövető által jogosulatlanul szerzett adat valamely már védett titok körébe tartozik, úgy az adott titok megsértését kriminalizáló a bűncselekmény hívandó fel.

A bűncselekmény tevékenységi tárgya az adat. Ez szerepelhet merev-, illetve hajlékony lemezen, lyukkártyán, lyukszalagon, COM- vagy CIM - mikrofilmen, de rögzíthetők optikai vagy akusztikai úton. Fontos kritérium az, hogy az ilyen adatok csak valamilyen technikai eszköz közbeiktatásával észlelhetők. Ugyankkor ez a tényállás szolgál a szoftverlopás büntetőjogi minősítésére is.

Az elkövetési magatartások kapcsán az mondható, hogy "nyitott törvényi tényállásról" van szó, azaz a törvényhozó tehát nem határozza meg az elkövetési magatartásokat. A jogosulatlan adatszerzés bármely - fentebb már megismert - módon történhet. A deliktum az adatok jogosulatlan megszerzéssel válik befejezetté. A bűnösség körében kiemelendő, hogy a bűncselekmény csak szándékosan követhető el. A tényállás a titoksértő bűncselekményekhez képest szubszidiárius

is megteremtődnek a kommunikáció legmodernebb lehetőségei. A tényállás kellően részletezi a modern elektronikus kommunikációs kapcsolat eszközeit.

Az **olasz** Btk. az *"Informatikai vagy teleinformatikai kommunikáció tiltott lehallgatása"* tényállás a következőkről rendelkezett:

"617. §-quater: (1) Aki csalárd módon lehallgat informatikai, teleinformatikai vagy több rendszert összekötő kommunikációt vagy korlátozza illetve megszakítja azt hat hónaptól négy évig terjedő szabadságvesztéssel büntethető.

(2) Ha súlyosabb bűncselekmény nem valósul meg az első bekezdés szerint büntethető az, aki bármely információközegen átmenő kommunikáció tartalmát egészben vagy részben másnak feltárja.

(3) Az (1) és (2) bekezdésben meghatározott bűncselekmények a sértett indítványára üldözendő.

(4) Az eljárás hivatalból indítandó és a büntetés egy évtől öt évig terjedő szabadságvesztéssel büntetendő,

1./ ha a cselekmény állam, közintézmény vagy közszolgáltató vállalat illetve közszükségletű informatikai vagy teleinformatikai rendszert érint,

2./ az a személy, aki köztisztviselő vagy közalkalmazott hatalmával visszaélve, hivatásával vagy szolgálatával járó kötelességét megszegve, valamint, aki rendszeroperátori minőségével visszaélve követi el,

3./ aki magánnyomozói hivatását akár jogellenesen gyakorolva követi el.

617. §-quinquies: (1) Aki a törvényben meghatározott eseteken kívül informatikai vagy teleinformatikai rendszerre vonatkozó kommunikáció lehallgatására, megszakítására, korlátozására alkalmas berendezést installál vagy több rendszert összekapcsol egy évtől négy évig terjedő szabadságvesztéssel büntethető.

(2) A 617. §-quarter szakasz (4) bekezdés eseteiben a büntetés egy évtől öt évig terjedő szabadságvesztés." [217]

---

[217] Leggi, decreti e ordinanze presidenziali ... id. közlöny 6-7. l. - saját fordítás

A **magyar** büntető törvénykönyv az 1998. évi LXXIII. törvénnyel, amely 1999. március 1-től hatályos a magántitok megsértésének esetére három konkuráló tényállást teremt, amelyek a távközlési rendszerek által közvetített számítógépes adatok védelmére *is* szolgálnak. Az első a 227/A. §-ban tilalmazott a *jogosulatlan titkos információgyűjtés.*

(1) Az a hivatalos személy, aki bíró vagy igazságügyminiszter engedélyéhez kötött titkos információ gyűjtést ill. a be. során bírói engedélyhez kötött titkos adatszerzést engedély nélkül végez vagy túllépi, bűntettet követ el és 5 évig terjedő szabadságvesztéssel büntetendő.
(2) Az (1) bekezdés szerint büntetendő, aki bíró vagy igazságügyminiszter engedélyéhez kötött titkos információszerzést elrendel vagy engedélyez, anélkül, hogy erre jogosult lenne.
(3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekmény jelentős érdeksérelmet okoz.

A magyar Alkotmány 59. §-a biztosítja a magánlakás és a magántitok védelmét az állampolgárok számára. A titkos információgyűjtés az állampolgárok jogaiba történő erőteljes beavatkozás.

Éppen emiatt külön törvényekben meghatározott szervezetek végezhetik, felderítési és bűnüldözési célból és bírói engedély alapján. Ilyen törvények: a nemzetbiztonsági szolgálatról szóló 1995. évi CXXV. tv., a rendőrségről szóló 1994. évi XXXIV. tv., a honvédelemről szóló 1993. évi CX. tv., valamint a vámjogról, vámeljárásról és vámigazgatásról szóló 1995. évi C. tv.

A bűncselekmény tárgyi oldalán értékelt elkövetési magatartások áttekintése:
- az engedélyhez kötött információgyűjtést a törvényben meghatározott engedély nélkül végzi,
- van ugyan engedélye, ám ezen engedély kereteit túllépi (a célszemély lakását átkutathatja, ám az elkövető lehallgató berendezést is telepít, vagy az e tevékenység alkalmazásának idejét meghaladóan végzi ezt), illetőleg

- a titkos információgyűjtést jogosulatlanul elrendeli, illetve engedélyez, pl. a távközlési rendszerek útján továbbított közlés tartalmának megismerése mindig engedélyhez kötött.

A bűncselekmény alanya: az (1) bekezdésben írt magatartást csak hivatalos személy követheti el, azaz a cselekmény delicta propria.

A magyar Btk. a hivatalos személyek közé vonja:

a. az országgyűlési képviselőt,

b. a köztársasági elnököt,

c. a miniszterelnököt,

d. a Kormány tagját, a politikai államtitkárt,

e. az alkotmánybírót, a bírót, az ügyészt,

f. az állampolgári, és a nemzeti és etnikai kisebbségi jogok országgyűlési biztosát, az állampolgári jogok országgyűlési biztosát és általános helyettesét, valamint a külön biztosokat,

g. a helyi önkormányzati testületek tagját,

h. a közjegyzőt,

i. az önálló bírósági végrehajtót,

j. az alkotmánybíróságnál, a bíróságnál, ügyészségnél, államigazgatási szerveknél, önkormányzati igazgatási szervnél, az Állami Számvevőszéknél, a Köztársaság Elnöki Hivatalánál, az Országgyűlés Hivatalánál szolgálatot teljesítő személyt, akinek a tevékenysége a szerv rendeltetésszerű működéséhez tartozik,

k. jogszabály alapján közhatalmi, államigazgatási feladatokkal megbízott szervnél, testületnél azt a személyt, aki közhatalmi, államigazgatási feladatot lát el (Btk. 137. § 1. pont).

A (2) bekezdés esetében elméletileg nem kizárt a hivatalos személyek körén kívül eső elkövető, ám a gyakorlatban a titkos információgyűjtést elrendelő, engedélyező tipikusan hivatalos személy.

A bűncselekmény csak szándékosan követhető el.

A minősített esetben említett "jelentős érdeksérelem", akkor hívható fel, amikor az elkövető a sértettnek jelentős anyagi, egzisztenciális avagy erkölcsi hátrányt okoz. A jelentős érdeksérelem a sértett szemszögéből vizsgálandó.

Illusztrációként lássuk a *rendőrségi törvény*nek az információgyűjtésre vonatkozó rendelkezéseit:

a. bírói engedélyhez nem kötött:

- az informátor alkalmazása,
- a gyanúsított és hozzá kapcsolódó személy valamint a bűncselekménnyel kapcsolatba hozható helyiség, épület, más objektum, terep-útvonalszakasz, jármű, esemény megfigyelése, információ gyűjtése, hang, kép, egyéb jel vagy nyom rögzítése,
- bizonyításhoz - sérülés v. egészségkárosodást nem okozó - csapdát alkalmazhat stb. ... (64. §)

b. bírói engedélyhez kötött információgyűjtés:

- magánlakást titokban átkutathat (titkos kutatás), az észlelteket technikai eszközzel rögzítheti,
- magánlakásban történteket technikai eszköz segítségével megfigyelheti, rögzítheti,
- levelet, egyéb postai küldeményt, valamint a telefonvezetéken vagy azt helyettesítő *távközlés rendszerek útján továbbított közlés tartalmát megismerheti, rögzítheti.* (69. §)

A különleges eszköz alkalmazását az engedélyt kérő nyomozó hatóság székhelye szerint illetékes helyi bíróság elnöke engedélyezi, és ennek időtartama legfeljebb 90 nap lehet, amely újabb 90 napra meghosszabbítható (71. §). A kérelemre a bíró végzéssel határoz 72 órán belül. Ha ez késedelemmel jár - sürgősségi elrendelés történik a nyomozó hatóság vezetője által (ezzel együtt bírósághoz kell fordulni).

A számítógépes hálózatokon (extra-, intra- illetve Interneten) keresztül menő elektronikus levelezés (e-mail) megismerése vagy rögzítése tehát bírói engedélyhez kötött.

A második bűncselekmény a 178/A. §-ban említett *a magántitok jogosulatlan megismerése.*

(1) Aki magántitok jogosulatlan megismerése céljából
a./ másnak a lakását, egyéb helyiségét vagy az ezekhez tartozó bekerített helyet titokban átkutatja,
b./ másnak a lakásában, egyéb helyiségében vagy az ezekhez tartozó bekerített helyet titokban átkutatja, technikai eszköz alkalmazásával megfigyeli, illetve rögzíti,
c./ másnak közlést tartalmazó zárt küldeményét felbontja vagy megszerzi és annak tartalmát technikai eszközzel rögzíti,
d./ távközlési berendezés útján másnak továbbított közleményt kifürkész, és az észlelteket technikai eszközzel rögzíti,
bűntettet követ el, és öt évig terjedő szabadságvesztéssel büntetendő.
(2) Az (1) bekezdés szerint büntetendő, aki az (1) bekezdésben meghatározott módon megismert magántitkot továbbít vagy felhasznál.
(3) A büntetés kettőtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt
a./ hivatalos eljárás színlelésével,
b./ üzletszerűen,
c./ bűnszövetségben,
d./ jelentős érdeksérelmet okozva követik el.

Ezt a bűncselekményt csak *magánszemélyek* követhetik el. Az általuk végzett jogosulatlan tevékenységet, az ilyen cselekménnyel megismert magántitok továbbítását vagy felhasználását rendeli büntetni.

A bűncselekmény tárgya: a magántitok, azaz a sértett vagy az által kialakított szűk körben ismert olyan tény, adat, körülmény, amely személyére, vagyoni helyzetére, családi körülményeire stb. vonatkozik és ezek megőrzéséhez méltányolható érdeke fűződik.

A bűncselekmény akkor valósul meg, ha az elkövető a magántitok megismerése céljából más lakását, egyéb helyiségét vagy az ezekhez tartozó bekerített helyet titokban átkutatja.

Ha az "elektronikus betörés" nem nyer önálló tényállást, úgy de lege ferenda a Btk. 178/A. (1) bekezdését ki kellene egészíteni *a belépési/hozzáférési kóddal védett számítógépek* esetével, hiszen számítógépeink is őrizhetnek magántitkokat. Ez a módosítás védelmet biztosít a titokgazdának akkor is, ha számítógépe más személyek (munkatársak, ügyfelek stb.) számára is nyitott, közös helyiségben (pl. tipikusan irodában, ügyféltérben) fellelhető.

A belépési/hozzáférési kóddal védett számítógép nem minden esetben van jelen a büntetőjog által védett, lokalizálható helyiségben vagy ahhoz tartozó bekerített helyen (pl. a hordozható számítógépek esetében.)

A bűncselekmény elkövetési magatartásai közül a d. pontban értékelt tevékenységet kell ehelyütt kiemelnünk: a távközlési berendezés útján továbbított közlemény kifürkészése és technika eszközzel történő rögzítése a büntetendő cselekmény.

A bűncselekmény tehát megvalósítható a telefon, faxon, telexen, rádión, géptávírón továbbá az *elektronikus adatfeldolgozásra alkalmas hálózatokon átmenő e-mailen* küldött közlemények (levelek, üzenetek stb. akár írásban, rajzban, gyorsírási jellel, titkosírással írt formában). A közlemény kifürkészése felölel minden olyan magtartást, amelynek célja a közlemény tartalmának jogosulatlan megismerése.

A bűncselekmény alanya - hivatalos személy kivételével - bárki lehet. Hivatalos személy a fentebb írt "jogosulatlan titkos információgyűjtés" bűntettéért felel.

A minősített eset valósul meg, ha az elkövető az (1) bekezdésben meghatározott módon megismert magántitkot harmadik személynek, a jogosult hozzájárulása nélkül továbbít vagy saját céljára felhasznál.

- Hivatalos eljárás színlelése állapítandó meg, ha az elkövető olyan látszatot kelt, ténykedése megkönnyítése végett, mintha az hivatalos eljárás keretében történne.

- Üzletszerűen követi el a bűncselekményt, aki hasonló jellegű bűncselekmények révén rendszeres haszonszerzésre törekszik (Btk. 137. § (9) bekezdés).
- Bűnszövetség pedig akkor létesül, ha két vagy több személy bűncselekményeket szervezetten követ el vagy ebben megállapodik (Btk. 137. § (7) bekezdés). E definícióhoz hozzátehetjük azt, hogy ezen személyeknek legalább egy bűncselekmény kísérletét meg kell valósítaniuk, feltéve, ha a bűncselekmény előkészülete nem büntetendő.
- A jelentős érdeksérelem a sértett szemszögéből vizsgálandó. Ez a sérelem lehet, vagyoni, erkölcsi vagy a sértett más méltányolható érdeke.

A harmadik bűncselekmény a 178. §-ban szabályozott *levéltitok megsértése*, amely 1999-ben átalakul és ennek eredményeképpen a tényállás szubszidiáriussá válik.

"178. § (1) Aki másnak közlését tartalmazó zárt küldeményét, a tartalmának megismerése végett felbontja, megszerzi vagy ilyen célból illetéktelen személynek átadja, úgyszintén aki távközlési berendezés útján továbbított közleményt kifürkész, ha súlyosabb bűncselekmény nem valósul meg vétséget követ el és pénzbüntetéssel büntetendő.

(2) A büntetés egy évig terjedő szabadságvesztés, közérdekű munka vagy pénzbüntetés, ha az (1) bekezdésben meghatározott bűncselekményt foglalkozás vagy közmegbízatás felhasználásával követik el.

(3) A büntetés

a./ két évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekmény,

b./ bűntett miatt három évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős érdeksérelmet okoz."

Az elkövetési magatartások közül a távközlési berendezés útján küldött közlemény kifürkészése érdemel említést.

A levéltitok megsértése csak akkor alkalmazható, ha súlyosabb bűncselekmény nem valósul meg, vagyis ha magánszemély és nem titkos eszközökkel fürkészi ki a távközlési rendszer útján továbbított közleményt.

Ha hivatalos személy, és nem titkos eszközökkel követi el a cselekményt, akkor a hivatali visszaélés (Btk. 225. §) hívható fel, feltéve, ha az ott írt "előny szerzése vagy hátrány okozása" fennáll. Az ezzel előidézett és a sértett szemszögéből vizsgálandó "jelentős érdeksérelem" súlyosító körülményként nyerhet értékelést.

A magyar büntető törvénykönyv további titoksértő tényállások találhatók, amelyekben a "távközlési rendszerek" nem szerepelnek nevesítve. Az államtitok (Btk. 221. §), a szolgálati titok (Btk. 222. §), az üzleti titok (Btk. 300. §), a banktitok (Btk. 300/A. §) megsértése megvalósítható az adott hivatal, más intézmény, gazdasági egység, pénzintézet számítógépes rendszerébe történő jogosulatlan belépéssel, vagy belépési jogosultság birtokában, ám a védett adatállományhoz illetéktelenül hozzáférve, továbbá távközlési vagy más azt helyettesítő rendszerek lehallgatásával.

Az *államtitoksértés* (Btk. 221. §) bűncselekménye megvalósítható - a fenti eszközcselekmények bármelyikével (is) - az államtitok jogosulatlan megszerzésével, az elkövető tudomására, birtokába jutott államtitok jogosulatlan felhasználásával, illetéktelen személy részére történő hozzáférhetővé vagy illetékes személy részére történő hozzáférhetetlenné tétellel.

- A megszerzés olyan szándékos magatartást jelent, amelynek során az elkövető a számítógép memóriájában vagy adathordozón tárolt és államtitkot képező információt (adatállományt) jogosulatlanul megismer, átmásolja azt az általa kijelölt háttértárolóra, adathordozóra, vagy elektronikus üzenetet, más közlést lehallgat stb.
- Az illetéktelen személy számára hozzáférhetővé tétel szintén szándékos magatartást feltételez. Az elkövető államtitkot képező adatállományt megjelenít egy monitoron, kinyomtatja egy papírlapra, olyan helyen, ahol illetéktelen személy megfordul, azzal a céllal, hogy az megismerhesse, valamint elküldi e-mailen, elérhetővé teszi az Interneten stb.

- Az illetékes személy számára hozzáférhetetlenné tétel olyan szándékos magatartásokat ölelnek fel, mint pl. az államtitkot képező adatállomány törlése, módosítása, továbbá az illetékes személy elől történő "elrejtés" (hozzáférési kóddal védetten).

Az 1 évtől 5 évig terjedő szabadságvesztéssel fenyegetett alapeseten túl minősített eseteket is szabályoz a törvényünk. Súlyosabb értékelendő a bűncselekmény és ezáltal 2-től 8 évig terjedő szabadságvesztés büntetés kiszabására nyílik lehetőség, ha ezen magatartásokat "különösen fontos államtitokra nézve" követik el, továbbá az államtitoksértés "súlyos hátrányt" okozott (pl. a nemzetközi gazdasági vagy politikai kapcsolatokban), továbbá 5 évtől 15 évig terjedő szabadságvesztés büntetéssel fenyegetett, ha az államtitok illetéktelen külföldi személy részére válik hozzáférhetővé.

Az államtitoksértés szándékos és gondatlan elkövetése, továbbá a minősített esetek előkészülete is büntetni rendelt.

A *szolgálati titoksértés* (Btk. 222. §) bűncselekménye körébe tartozik e titokfajta jogosulatlan megszerzése, az elkövető tudomására, birtokába jutott szolgálati titok jogosulatlan felhasználása, illetve illetéktelen személy részére történő hozzáférhetővé tétel.

A minősített esetek között szerepel az, ha a szolgálati titoksértés "súlyos hátrányt okoz" (ez 3 évig terjedő szabadságvesztéssel sújtható) vagy ha a szolgálati titok vagy katonai titok illetéktelen külföldi személy részére válik hozzáférhetővé. Előbbi esetben 1 évtől 5 évig, utóbb 2 évtől évig terjedő szabadságvesztéssel is büntethetők az elkövetők.

Az *üzleti titok megsértése* (Btk. 300. §) bűncselekmény haszonszerzés végett vagy másnak hátrányt okozva történő megszerzését, felhasználását, nyilvánosságra hozását 3 évig terjedő szabadságvesztéssel bünteti. Az üzleti titok fogalmát a Btk. a tisztességtelen piaci magatartásról szóló törvény meghatározását (1990:LXXXVI. tv.) alapul véve definiálja: ez alapján üzleti titok "minden olyan tény, információ, megoldás vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik."

A *banktitok megsértését* a banktitok megtartására köteles személy, - aki elméletileg nemcsak banki alkalmazott lehet, hanem más személy is, aki pl. hivatalos személyként, véletlenül, netán tévedésből ilyen titokhoz hozzájutott személy követheti.

Elkövetési magatartásként a törvény az illetéktelen személy részére hozzáférhetővé tételt fogalmazza meg.

6. 9. Az adatvédelem - a privacy és az információszabadság

Az elektronikus adatfeldolgozásra került adatok jogosulatlan kifürkészése, megszerzése kapcsán szólnom kell az információ szabad áramlását biztosító és az ezzel szorosan összefüggő a magánszférát védő jogszabályokról. Míg a társadalom és a gazdaság hatékony és eredményes működéséhez információra van szükség, addig az információ szabad áramoltatása, felhasználása egy - egy szférában nemcsak politikai, és üzleti érdekeket, hanem magánszemélyek érdekeit is sértheti vagy veszélyeztetheti. Az információszabályozásról szóló jogszabályok a jogforrási hierarchia több szintjén helyezkednek el:

a. az általános rendelkezéseket tartalmazó törvények (az Alkotmánytörvények),
b. a speciális törvények:
ba. az információszabadság (Freedom of Information - FOI -) törvényei,
bb. a magánszféra- (Privacy) és az adatok védelmére (Data Protection Act) szolgáló törvények,
c. egyes részterületet átfogó jogszabályok (pl. a népszámlálás, a statisztikai adatfeldolgozás szabályait körülíró jogi normák).

Svédországban már 1776-ban a sajtószabadságról szóló törvény kinyilvánítja, hogy hivatali dokumentumokat kérésére bárkinek rendelkezésére kell bocsátani, illetve azokról másolatot lehet készíteni vagy hitelesített másolatot lehet kiadni. Ezzel elsőként fogalmazzák meg az *aktanyilvánosság* alkotmányos elvét.

Ezt a törvényt tekinthetjük az információszabadságról szóló törvény ősének.[218]

Az információkhoz való szabad hozzáférést biztosító törvényeket a közigazgatás igazságosságának, tisztességének valamint hatékonyságának kontrollálása végett hívják életre. Emellett valljuk, hogy minden állampolgár számára biztosítani kell a tájékozódáshoz illetve a tájékoztatáshoz való jogot. Ez felel meg a demokrácia egyik alapelvének, ennek hiányában a közügyekben való részvétel (is) elképzelhetetlen. Az *információszabadságról* szóló törvények az információhatalom megosztásának elvét, és gyakorlati megvalósulását rögzíti. Egyfelől állampolgári jogként deklarálva az információszerzés jogát, másfelől a hivatalok kötelességévé teszik az információszolgáltatást, meghatározva azt, hogy milyen információk, mennyi idő alatt hozhatók nyilvánosságra valamint a kiadás megtagadása ellen az információkérőnek milyen jogorvoslati lehetősége van. Vagyis az államhatalom-, és igazgatás nem gyűjthet korlátlanul az állampolgárokról adatot illetve azokkal nem rendelkezhet önkényesen, továbbá nem titkolhat el közérdekű információkat az állampolgárok elől. (Pl. Finnországban 1951., az Amerikai Egyesült Államokban 1967., Norvégiában, Dániában 1970., Franciaországban 1978., Hollandiában 1980., Kanadában, Ausztráliában és Új-Zélandon 1982., Görögországban 1986-ban.) Az Egyesült Államokban az információszabadságról szóló törvény mellett további jogszabályok konkretizálnak állampolgári jogokat A "Government in the Sunshine" (A kormányzati nyilvánosságról szóló) törvény kijelöli a különféle közigazgatási fórumokon való szabad részvétel lehetőségét, azok nyilvánosságát. E tárgykörben a szövetségi szintű szabályokat rögzít a "Federal Advisory Commitee Act". Az USA-ban e törvények alapján nyernek nyilvánosságot néhány nukleáris erőmű biztonságáról, környezeti sugárzásairól, egyes gyógyszerek kétes mellékhatásairól, közéleti emberek adóiról,

---

[218] Jogi informatika. (Szerkesztők: Hársfalvi Rezső - Katona Tamás - Kovacsics József - Péntek László. Szerk. Elnök: Kovacsicsné Nagy Katalin.) ELTE. Budapest, 1996. 67.l.

illegális fegyverexportról, pártok számára juttatott illegális pénzekről, korrupció gyanúkról stb. A *privacy* és az *adatvédelmi* törvények az információszabadságról szóló törvények "ikertestvérei". E törvények együttesen teremtik meg a modern társadalom demokratikus információs egyensúlyát, gyakorlatát, vagyis ezek a szabad információáramlás és az adatvédelmi érdekek kiegyenlítésére hivatottak. Az információhoz való hozzáférés, valamint az adatvédelemhez való jog geometriai síkban egymásbafonódó homorú és a domború alakzatokként ábrázolhatnók. Eme egyensúly megtalálása igen kényes kérdés.

A korlátok kijelölése természetesen nem független az adott ország demokratikus berendezkedésének, intézményrendszerének, a személyiségvédelemnek fejlettségétől, a társadalmi tradícióktól, az állampolgárok egyéni érzékenységétől. Az információktól való indokolatlan megfosztás felerősíti az adatok ellenőrizetlen "feketekereskedelmét", és növeli a számítástechnikai rendszerek veszélyeztetettségét. A másik véglet az adatokhoz való hozzáférés teljes körű szabadsága, amely valójában sohasem létezik, létezhet hiszen az állam- és államhatalom nem fedi fel, mert nem is teheti valamennyi általa ismert információt illetve annak tartalmát. E - jelen történelmi viszonyok közepette - kissé naiv elképzelés kapott teret egy a kilencvenes évek végén életrehívott Electronic Frontier Foundation (Elektronikus Határ Alapítvány) nevű szervezet alapítóüzenetében: "biztosítjuk a számítógépkalózok bíróság előtti védelmét a demokrácia tiszteletbe tartásának elve alapján, és attól a meggyőződéstől vezérelve, hogy mindenkinek joga van hozzájutni az információhoz."[219]

Az információszabadsághoz való jogosultságot, ezzel együtt az adatvédelem megteremtését szorgalmazó nemzetközi közvélemény egyre erősödő nyomása, valamint a külön utakon induló nemzeti törvényalkotási hullám arra ösztönözte a (legkülönfélébb) nemzetközi szervezeteket, hogy e témában (is) ajánlásokat, irányelveket dolgozzon ki, amelyben részint összegzik az eddig felhalmozott

---

[219] idézi a Jogi Tudósító XXII.évf. 21-22-i száma (1991. november) 21. lapon a L'Unita 1991. március 13. írását.

jogalkotási és jogalkalmazási tapasztalatokat, részint a majdani törvényhozás számára fogalmazták meg az iránymutató elveket.

E számtalan nemzetközi dokumentumok között jelentőségét tekintve kiemelkedik az **OECD** Miniszterek Tanácsa által 1980-ban kibocsátott Ajánlása és az **Európa Tanács** 1981-es Adatvédelmi Konvenciója, valamint legújabban az **ET** (99) 5. sz. Ajánlása.Bár e két dokument bár eltérő célkitűzésből születik, azonban köztük az alapelvek megfogalmazásában hasonlóság mutatkozik. Az OECD direktívája a nemzetközi adatáramlás korlátait felszámolására az ET Ajánlás az emberi jogok védelmére helyezi a hangsúlyt. Ezen alapelvek az alábbiak:

- a tisztességes és törvényes adatgyűjtés elve,
- az adatminőség biztosításának elve,
- a célhoz kötöttség elve, ezen belül - a célhoz szükséges minimális mennyiségű adat gyűjtése elve, - a célhoz szükséges minimális feldolgozás elve, - a célhoz szükséges minimális időtartamú adattárolás elve, - a nyilvánosság elve, - a személyes hozzáférés elve, ezen belül a tájékozódáshoz, a betekintéshez, a helyesbítéshez vagy törléshez való jog, - a technikai adatbiztonsághoz való jog.[220]

Az **ET. (89) 9. sz. Ajánlásáról** rendezett 1992. évi *würzburgi konferenciájának* ajánlásában megállapítja, hogy "a magánélet érdekvédelmének jelentőségét az információs korszak elismeri, de ellensúlyozza is információk szabad forrásának és áramlásának törvényes érdekei által. Ezek az érdekek magukban foglalják az állampolgárok jogait az információhoz jutáshoz, információkat önmagukról, amit másoktól szereztek, de legális eszközök útján. A büntetőjogi rendelkezéseket csak abban az esetben célszerű felhasználni, amikor a polgári jog vagy az adatvédelmi jog nem gondoskodik megfelelően a törvényes orvoslásról..... Büntetőjogi rendelkezések a magánélet területén- akkor vehetők igénybe, ha a cselekmények súlyos jogsértést okoztak, különösen ha rendkívül kényes adatokat érintettek vagy olyan bizalmas információkat, amelyeket a jog védelemben részesíti,

---

[220] Dr. Kertész Imre - Dr. Pusztai László: A komputerbűnözés és az információs technológiával kapcsolatos egyéb bűnözési fajták. ÜÉ. 29. 1993.4. 17-18.l.

- világosak és pontosak legyenek, kerüljék az általános klauzulákat, különösen a magánéletre vonatkozó anyagi jog területén,
- tegyenek különbséget a büntetőjogi felróhatóság, a bűnösség és a gyanakvás szintje között,
- legyenek körültekintőek különösen a szándék lényegét illetően,
- a személyes adatok ugyanolyan védelméről gondoskodjanak, mint amilyen védelem illeti meg a gazdasági érdekeket, és- vegyék figyelembe néhány bűncselekménytípusnál a sértett kívánságát, tekintettel a büntetőeljárás megindítására." [221]

Hazánkban az elmúlt négy évtized szocialista időszakának jellemzője az volt, hogy az állam(igazgatás) a magánszemélyek adatait korlátlanul gyűjti, gyűjtheti, és bitorolja, viszont a közérdeklődésre számot tartó információk az állampolgárok elől elzárva vannak. Tehát a nyugat - európai törekvésekkel ellentétes tendencia jellemzi a hazai, és eltérő mértékben más szocialista országok gyakorlatát. A politikai - gazdasági rendszerváltást követően az Alkotmánybíróság az alapjogok érvényesítése érdekében kifejtett következetes ítélkezési gyakorlatának köszönhetően a magántitok és személyes adatok védelmének nemzetközi jogi standard-jei bekerülnek a hazai jogi gondolkodásba, és az adatvédelmi törvény elméleti kimunkálásához elévülhetetlen segítséget jelentenek. Az alkotmánybírósági judikatúrából - témánk szemszögéből - az alábbi határozatokat emelem ki:- A 20/1990. (X.4.) sz. határozatában leszögezi, hogy a magántitok és a személyes adatok védelméhez való jog nem abszolút jog, törvény kivételesen elrendelheti a magántitok és a személyes adat kiszolgáltatását és meghatározhatja a

---

[221] "AIDP Konferencia a számítógépes bűnözésről és más információs technológia ellen elkövetett bűncselekményekről" (kézirat magyar nyelvű fordításban 8. l. II. pont), továbbá

Dr. Nagy Zoltán: Konferencia .... id. mű 102-104.l.

felhasználásának módját is. Bármely jogszabály, amely személyes adat felvételéről, gyűjtéséről, tárolásáról, rendezéséről, továbbadásáról, nyilvánosságra hozataláról, megváltoztatásáról, a további felhasználásáról rendelkezik csak akkor felel meg az Alkotmány 59. § - nak, ha az érintett személy számára garanciát biztosít jogai gyakorlásához. [222]- A 15/1991. (IV.13.) sz. határozatában az Alkotmánybíróság a sokat bírált személyi szám használatának kapcsán kifejti, hogy az információs önrendelkezési jog gyakorlásának feltétele és legfontosabb garanciája az adatgyűjtés célhoz kötöttsége, valamint az adattovábbítás, és nyilvánosságra hozás törvényi korlátozása. A határozat kiemeli azt, hogy "az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája a célhoz kötöttség. Ez azt jelenti, hogy személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célra szabad. Az adatfeldolgozásnak minden szakaszában meg kell felelnie a bejelentett és közhitelűen rögzített célnak.... A célhoz kötöttségből következik, hogy a meghatározott cél nélküli, "készletre", előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és tárolás alkotmányellenes." [223]

- A 29/1994. (V.20.) sz. határozatában hangsúlyozza, hogy a kétféle személyazonosító jelrendszer (ti. személyi szám és az ún. ágazatspecifikus azonosítószám) használata ugyanarra a célra "általában véve is az információs önrendelkezési jog lényeges tartalmának a sérelmét jelenti".[224]Ugyanis a kétféle azonosítójel alkalmazása ugyanazon célra megkönnyíti az elektronikus adatfeldolgozó rendszerek összekapcsolása révén az állampolgárok adatainak elérését, ugyanakkor megnehezíti vagy lehetetlenné teszi azt, hogy az adott személy kövesse és ellenőrizze az adatfeldolgozás folyamatát. Ezt a felfogást erősíti meg a 46/1995. (VI. 30.) sz. határozatában az Alkotmánybíróság .[225]

- A 34/1994. (VI. 24.) sz. határozat elvi éllel állapítja meg, hogy "az információszabadság, a közhatalom gyakorlásának nyilvánossága, az állam és a

---

[222] Alkotmányos elvek és esetek (Kézikönyv). Kiadja: Constitutional & Legislative Policy Institute (COLPI) 1996. 604.l.
[223] Alkotmányos elvek ... id. mű 605.l.
[224] Alkotmányos elvek ... id. mű 607.l
[225] Alkotmányos elvek ... id. mű 607.l

végrehajtó hatalom tevékenységének átláthatósága, ellenőrizhetősége feltétele a bírálat jogának, a kritika szabadságának, a szabad véleménynyilvánításnak".[226] A határozat kiemeli, hogy a kontroll alatt tartott végrehajtó hatalom a "demokratizmus alapköve".

- A 60/1994. (XII. 24.) sz. határozatában a testület leszögezi, hogy szabad véleménynyilvánítás joga, mint anyajog magában foglalja a közérdekű adatok megismerésének jogát is. Emellett a személyes adatok védelméhez való alapjog, és a közérdekű adatok megismeréséhez való alapjogot csak egymásra tekintettel lehetséges értelmezni. A határozat indokolása szerint "ez természetes, hiszen az információs önrendelkezés és az információszabadság a személy autonómiájának két, egymást kiegészítő feltétele".[227]

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvény 1992-ben lép hatályba. Ennek alapján az 1993:XVII. törvénnyel teremtik meg az adatok büntetőjogi védelmét.

"Jogosulatlan adatkezelés
177/A. § (1) Az az adatkezelő vagy adatfeldolgozó aki
a./ jogosulatlanul vagy a céltól eltérően személyes adatot kezel;
b./ személyes adatot jogellenesen továbbít vagy nyilvánosságra hoz;
c./ személyes adatok kezelésére vonatkozó bejelentési kötelezettségét nem teljesíti;
d./ személyes adatot az arra jogosult elől eltitkol;
e./ kezelt személyes adatot meghamisít;
f./ közérdekű adatot eltitkol vagy meghamisít, vétséget követ el, és egy évig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő."

Ez a tényállás keretdiszpozíció, amelynek tartalmát a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992:LXIII. tv. (továbbiakban: Atv.) rendelkezései teszik ki. A bűncselekmény jogi tárgya az

---

[226] Alkotmányos elvek ... id. mű 617.l.
[227] Alkotmányos elvek ... id. mű 621.l.

adatkezelés biztonságához fűződő társadalmi érdek. Tevékenységi tárgya az adat, amely minőségét tekintve: a tényállás a. - e. pontjában a személyes adat és az f. pontjában a közérdekű adat. Személyes adat az Atv. értelmező rendelkezése szerint: meghatározott természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Azon adatok, amelyek nem azonosíthatók az érintettel, nem részesülnek jogi, így büntetőjogi védelemben. A nemzetközi joggyakorlatban az adatokat akkor is anonimizáltnak tekinti, ha személyes jellegük csak aránytalan technikai, és anyagi eszközök révén lenne helyreállítható.[228]

A közérdekű adat fogalmát negatív módon definiálja az Atv., azaz az állami vagy helyi önkormányzati feladatot ellátó szerv kezelésében levő, a személyes adat fogalma alá nem eső, és a törvényben meghatározott kivételek körébe nem tartozó adat. A személyes adatok körét több törvény állapítja meg, így a büntetőeljárásról szóló 1973. évi I. tv., a rendőrségről szóló 1994. évi XXXIV. tv., az ügyészségi szolgálati viszonyról és az ügyészségi adatkezelésről szóló 1994. évi LXXX. tv., a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. tv., a határőrizetről, és határőrségről szóló 1997. évi XXXII. tv. stb.

A tárgyi oldalon értékelt elkövetési magatartások áttekintése:

a. a jogosulatlanul vagy a céltól eltérő személyes adatkezelés. Az adatkezelés fogalmára is a Atv. ad magyarázatot. E szerint az adatkezelés az alkalmazott eljárástól függetlenül a személyes adatok felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt), adatkezelésnek számít az adatok megváltoztatása, és további felhasználásuk megakadályozása is. De jogosulatlan az adatkezelés akkor is, ha ahhoz az érintett nem járult hozzá, továbbá ha az adatkezelés törvény vagy önkormányzati rendelet hiányában történt, valamint ha az adatkezelést nem az arra feljogosított személy végzi stb. Céltól eltérő az adatkezelés, ha az adatkezelés céljához szükséges mennyiségű vagy minőségű adat kezelése történik vagy ez a tevékenység a meghatározott időt túllépi.

---

[228] Dietz Gusztávné: Adatvédelem - adatbiztonság. Novorg, Budapest, 1995. 65.l.

Tilalmazott tehát az adatkezelés céljával össze nem férő személyes adatot felvétele, tárolása, továbbítása stb.

b. Személyes adatot jogellenesen továbbítása vagy nyilvánosságra hozatala. Jogellenes az adattovábbítás akár belföldre, akár külföldre, ha az érintett hozzájárulásának hiányában valósult meg, vagy ha az adattovábbítást a törvény kizárja. A nyilvánosságra hozatal megvalósulhat aktív vagy passzív módon, amelynek eredményeképpen a személyes adat illetéktelen tudomására jut.

c. A személyes adatok kezelésére vonatkozó bejelentési kötelezettségét nem teljesítése. Az Atv. előírja, hogy az érintettel már az adatkezelés első fázisában, vagyis az adatfelvételkor közölni kell az adatszolgáltatás önkéntes vagy kötelező jellegét, és az azt elrendelő jogszabályt, az adatkezelés célját, és az adatokat kezelőt is.

d. A személyes adatnak az arra jogosult elől történő eltitkolása. Az Atv. kiköti továbbá, hogy az érintett tájékoztatást kérhet személyes adatai kezeléséről, céljáról, jogalapjáról, időtartamáról és arról, hogy kik és milyen célból kapták vagy kapják meg az adatait. Az adatkezelő a legrövidebb időn, de 30 napon belül köteles e tájékoztatást megadni. Ám tájékoztatási kötelezettség kizártságát csak e törvény határozza meg. Ezek alapján az adatkezelő büntetőjogi felelősséggel tartozik, ha az érintett kérése ellenére az adattájékoztatási kötelezettségét azonnal vagy a 30 nap elteltével szóban vagy írásban megtagadja.

e. A kezelt személyes adat meghamisítása. A hamisítás módszere az adatkezelési eljárástól függ. Számítógépes adatkezelés esetén a - fentebb megismert - adathamisítási technikák jönnek szóba, így az adatok jogellenes módosítása, felülírása, kiegészítése stb.

f. A közérdekű adat eltitkolása vagy meghamisítása. A tényállás eme fordulata tevékenységi tárgy minőségében mutat eltérést az előzőektől. Továbbá a tevékenységi tárgy sajátosságából folyóan ama részletszabályban, miszerint az adatkezelő tájékoztatási kötelezettsége 15 napra korlátozódik.

A bűncselekmény ex officio indul. Ez a törvényi megoldás ellentétes a würzburgi konferencia ajánlásával szemben. Talán egy későbbi törvénymódosítás a magánindítványra büntetendő bűncselekmények közé sorolhatja.

A bűncselekmény alanya az 1999. évi LXXII. tv. hatálybalépése óta csak adatkezelő vagy adatfeldolgozó lehet. Adatkezelő az a személy, aki a személyes adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bíz meg. Adatfeldolgozó pedig az a személy, aki az adatkezelő megbízásából az adatkezelési műveleteket, technikai feltételeit végzi. Részesként más személyek is szóba jöhetnek. A bűnösség vizsgálatakor megállapítható, hogy a bűncselekmény csak szándékosan követhető el. A jogosulatlan adatkezelés bűncselekménye tipikusan magatartás tényállás. Befejezetté válik akkor, ha a tényállásban megfogalmazott magatartás akár aktív, akár passzív formában megvalósul. A stádiumok közül kiemelést igényel a kísérlet kizártsága azokban az esetekben, amikor a jogosulatlan adatkezelés mulasztással valósul meg pl. a személyes adatok kezelésére vonatkozó bejelentési kötelezettség nem teljesítése.

Az adatvédelemhez fűződő egyéni és egyben társadalmi érdeket sértő bűncselekmény a *különleges személyes adatokkal visszaélés.*

"177/B. § (1) Aki a személyes adatok védelmére vonatkozó jogszabályban meghatározott adatkezelése során tudomására jutott különleges adatot

a./ jogellenesen nyilvánosságra hozza;

b./ jogosulatlanul felhasználja vagy illetéktelen személy részére hozzáférhetővé teszi bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő.

(2) Aki különleges adatot maga vagy más részére jogosulatlanul megszerez, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő."

Ez a bűncselekmény tevékenységi tárgyában mutat eltérést az előzőtől. Különleges személyi adat a faji eredetre, a nemzeti, a nemzetiségi és az etnikai hovatartozásra, a politikai véleményre, pártállásra, a vallásos vagy más meggyőződésre, az egészségi állapotra, a kóros szenvedélyre, szexuális életre,

továbbá a büntetett előéletre vonatkozó személyes adatok. Különleges személyes adatra több törvényünk is utal:

A bűnügyi nyilvántartással kapcsolatban az 5/1979. (X. 14.) BM. rendelet kiterjed arra, akivel szemben büntetést szabtak ki, intézkedést alkalmaztak, vám- és deviza-szabálysértés miatt felelősségre vont személyekre, az előzetesen letartóztatottakra és az eljárási kegyelemben részesítettekre. Ezen adatok csak meghatározott szervek számára adhatók ki.

A statisztikáról szóló 1993. évi XLVI. tv. 8. § (4) bekezdése alapján a természetes személy faji eredetére, nemzeti, nemzetiségi, etnikai hovatartozására, politikai véleményére vagy pártállására, vallásos meggyőződésére, egészségi állapotára, kóros szenvedélyére, szexuális életére, valamint büntetett előéletére vonatkozó személyes adatot statisztikai célra csak az érintett természetes személy írásbeli beleegyezésén alapuló önkéntes adatszolgáltatása vagy törvény előírása alapján lehet gyűjteni.

A gyermek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. tv. 135. § (2) bekezdése szerint a gyermek, a szülő és más törvényes képviselő, a helyettes szülő és a nevelőszülő vagyoni helyzetére, egészségi állapotára és büntetlen előéletére vonatkozó adatok tartoznak a különleges személyes adatok körébe.

Az egészségügyi és hozzákapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVI. tv. 3. § a. pontja alapján az érintett testi, értelmi és lelki állapotára, kóros szenvedélyére, a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátóhálózat által észlelt, vizsgált, mért, leképzett vagy származtatott adat; továbbá az előzőekkel kapcsolatba hozható, az adatokat befolyásoló mindennemű adat, valamint a szexuális szokásokra vonatkozó adat egészségügyi adatnak tekintendő.

A bűncselekmény elkövetési magatartásai a titoksértő bűncselekmények tipikus elkövetési magatartásai. A bűncselekmény alanyainak köre eltér az alap- és a privilegizált esetekben. Az (1) bekezdésben tettesként csak az adatkezelő felel, a

(4) bekezdésben meghatározott magatartást bárki megvalósíthatja. Problémát vethet fel a (2) bekezdésben értékelt "maga vagy más számára megvalósuló jogosulatlan adatszerzés" elbírálása, annak fényében, hogy ez a tevékenység az (1) bekezdésben írt magatartásoknak előcselekménye is lehet. Ehelyütt azt kell vizsgálnom, hogy ez a "jogosulatlan megszerzés" milyen célból történik. E szerint, ha az adatkezelő a jogosulatlan adatszerzés célja az adat nyilvánosságra hozatala, jogosulatlan felhasználása vagy illetéktelen személy részére való hozzáférhetővé tétele akkor az (1) bekezdés kísérletének megállapítására sor kerülhet.

6. 10. A védett számítógépes programok jogosulatlan másolása, kereskedelme

A számítógépes környezetben elkövetett bűncselekmények egyik gyakori célpontja a szoftver. Egy szoftver elkészítése meglehetősen költséges beruházás, áruk magasak. Elismerendő az intenzív fejlesztés, a szakismeret, és a ráfordított nem kevés idő.

A számítógépes szoftverek fő fajtái az alábbiak:

a. a kereskedelmi programok a hagyományos kereskedelmi hálózatban beszerezhető programok. A kereskedő felel az eladásra kínált szoftver jogtisztaságáért. Nem ritkán keveredik a kereskedőknél a legális és az illegális (másolt vagy egyéb forrásból beszerzett) szoftver.

b. Az ún. osztott használatú (shareware) programok jellemzője az, hogy nem kerülnek a kereskedelem vérkeringésébe, hanem a szerző vagy az általa megbízott személy számítógépes hálózaton vagy valamilyen adathordozón terjeszti programját. A felhasználó általában teszteli az így kapott szoftvert, amelyért a tesztelési időn belül nem fizet, ám annak lejártát követően regisztráltatnia kell magát, mint szoftverhasználó, és a felhasználói díjat köteles megfizetni. A felhasználó által fizetett díj nem jelent más további jogosultságot (pl. terjesztés, másolás stb.) számára.

c. Az ún. szabad (freeware) program megszerzése (az Internetről, a szoftvergyártók által küldött ajándék CD stb.) ingyenes, ám a szerzők személyhez fűződő jogait köteles tiszteletben tartani, vagyis nem terjesztheti saját szerzőségének nyilvánítva a programot.

d. A nyilvános (public) programok szabadon terjeszthető, használható, sőt módosítható. Ebben az esetben a szerző lemondott mindenféle vagyoni illetőleg személyhez fűződő jogáról.

Az egyedi programok esetében a felhasználó speciális, testreszabott igényeit kiszolgáló rendel a szoftvergyártótól. A felhasználó, és a gyártó között létrejött szerződés részletesen tartalmazza a felek jogait és kötelezettségeit.

A számítógépes szoftvereket illegálisan beszerző vagy azzal kereskedő kalózoknak állandó és biztos profitot hozó piacot jelent az élénk kereslet, virágzik a "feketekereskedelem". A "vevők" viszont az olcsó ár fejében lemondanak a biztonságról. Hiszen az ellenőrizhetetlen forrásból származó szoftverek olyan vírusokat tartalmazhatnak, amelyek a felhasználóknak komoly károkat okozhatnak.

A visszaélések az alábbiakban csoportosíthatók:

a. a szoftverek hamisítása azok jogosulatlan másolását, terjesztését jelenti. E cselekmények tipikus célpontjai az operációs rendszerek, szövegszerkesztő- és táblázatkezelő programok.

b. Kereskedői visszaélések közé tartoznak azon esetek, amikor az eladók esetben a számítógépes szoftvereket jogosulatlanul másolják az értékesíteni kívánt merevlemezre, így a a számítógépek már feltöltve kerülnek értékesítésre (az egyébként legális szoftver árával megnövelve).

c. A (vég)felhasználói visszaélésnek tekinthető a legálisan beszerzett szoftvereknek az engedélyezettnél nagyobb számban (több gépen, nem a munkahelyen stb.) való felhasználása.

d. A csomagküldői visszaélések jelentik a jogosulatlanul szerzett (lopott, másolt stb.) szoftverek a sajtó hasábjain, az Inter-, intra- vagy extraneten vagy más módon (iskolai, faliújságon, falragaszokon, telefonon, e-mailen stb.) keresztül történő reklámozását, majd általában utánvételes értékesítését.

e. Az elektronikus úton megvalósuló visszaélés során a legálisan vagy az illegálisan beszerzett szoftvereket a hálózatokon, e-mailen stb. keresztül teszik hozzáférhetővé a kalózok. Ez a ún. hirdető-tábla kalózkodás.

A szoftverek illegális megszerzése, másolása, forgalmazása a szoftvergyártók többirányú érdekeit sértik, számukra tetemes anyagi, és nem utolsó sorban erkölcsi veszteséget okoz. Nem ritkán egyes szoftvergyártók piaci helyzetük erősítése, a konkurencia letörése céljából nyúlnak a szoftverkalózkodás nemtelen eszközéhez. A szoftverek illegális másolása, kereskedelme nem vitatható előnyökkel is jár a felhasználók számára, és ezek a keresletet fenntartják az illegális termékek iránt. Egy új szoftverrel - amelyet ha jogosulatlanul is szerez meg magának a felhasználó - az otthon végzendő munka hatékonyabbá és gyorsabbá válhat, ami gazdasági előnyöket is jelent. Kispénzű, kísérletező kedvű komputer - rajongók számára a számítógépes szoftverek árai megfizethetetlenek. (2000-ben egy-egy újabb, bonyolultabb játékprogram Magyarországon közel tízezer forintért kapható kereskedőknél. A hazai átlagfizetések megvásárlásukat nem teszik lehetővé, amiben a szoftvergyártók nem hibásak. Ezen eltúlzott árat, egy hamar, pl. hetek alatt avuló, kiismerhető játékért nem szívesen fizeti ki egy fiatal, inkább a jogsértő "szellemi viadalt" választja a program megszerzéséért. Avagy cserélgetik azokat egymás között. Ugyanakkor egy - egy új szoftver kipróbálásával a kalózok lépést tartanak a fejlődéssel, új ismeretre, szemléletre tehetnek szert. A hackerek "kinézik" maguk közül azt, aki legálisan jut a legújabb szoftverhez. A szoftverek tökéletes technikai védelme nem létezik. A szoftvergyártók számtalan technikai eljárással kísérleteznek, amelyek a hardvert teszik alkalmassá az adott program futtatásához, másrészt a szoftverek másolását akadályozzák. A biztonsági eljárások alkalmazása megdrágítja a terméket. Éppen ezért a szoftvergyártó cégek a nagyközönség számára készült, kommersz programokat általában már nem is védik, vagy csak a házilagos másolást kívánják megakadályozni. Csupán az egyedi felhasználói igényeket kielégítő programokat látják el teljes körű védelemmel.

Legújabban egyes számítógépgyártó cégek, így a Microsoft az általuk gyártott komputerekbe programot telepítve értékesítenek. Ezzel szorítják háttér annak lehetőségét, hogy a vevők illegális forrásokból szerezzék be a számítógép működtetéséhez szükséges szoftvereket. Ugyanezen cég a pénzhamisítás ellen bevált megoldásokkal (pl. vízjellel, speciális dombornyomású papírral, lézerrel a

lemez felületére gravírozott, hitelesítő hologrammal) teszik azonosíthatóvá a programot. A számítógép szoftverek jogtisztaságának ellenőrzésére nemzetközi szervezetet, a BSA-t (Business Software Alliance-t) hívják életre. A szervezet tagjai próbavásárlásokkal és házkutatásokkal igyekeznek kiszűrni a hamis szoftvereket. Egyes szoftver forgalmazó világcégek, így Novell saját teamet (az APG - Anti Piracy Group) is létrehozott termékei védelmére.

A számítógépes programok jogi megítéléséről élénk vita folyik a hetvenes évek elejéig, amikor a diszkusszió, ha nem is jut nyugvópontra, de berekesztődik. A polémia - amelyet röviden érintenem kell a büntetőjogi védelem megértéséhez - tárgya, hogy szabadalmazható-e a szoftver vagy sem. A szabadalmi védelem megadása mellett voksolók azzal érvelnek, hogy a szoftver végső felhasználását tekintve ipari jellegű termék, csak ipari - gazdálkodó szervezetek használják akkoriban és zömében ma is ez a jellemző. Ennek megfelelően az iparjogvédelem megadása indokolt. E felfogás ellenzői azt hozzák fel, hogy a szoftver nem valóságos anyagi termék, csupán logikai konstrukció, amire viszont azzal replikáznak a szabadalom hívei, hogy valamennyi új gyártási eljárás alapja egy új logikai ötlet. A lassan meddővé váló és elhúzódó elméleti(es) vitát - mint már annyiszor - a gyakorlat oldja meg. A hatvanas évek végéig a nagy számítógépgyártó cégek gépeikkel együtt értékesítik a programokat, mígnem 1969-ben az amerikai IBM-t a trösztellenes törvény rendelkezései alapján arra kényszerítik, hogy ezentúl a szoftvert külön értékesítsék. Mivel az inkriminált cég korábban a szoftver szabadalmazhatósága ellen foglal állást, így a szerzői jog elkötelezett híveként jelenik meg. Ez az ítélet meggyorsítja a számítógépes szoftver szerzői jogi elismerését. Az 1973. évi Európai Szabadalmi Egyezmény kinyilvánítja, hogy az elektronikus adatfeldolgozó berendezésekhez írott szoftverek nem tekinthetők találmánynak. Az Egyesült Államokban 1980-tól, míg Ausztriában 1984-től, illetve Németországban és Franciaországban 1985-tól terjed ki a szerzői jogi védelem a számítógépes szoftverekre. Ebből a törvényalkotási folyamból a jogi hagyományokhoz hozzánk közel álló német szabályozást emelem ki.

A **német** szerzői jogi törvényt 1990-ben módosítják, amelyben többek között a büntetőjogi rendelkezéseket is szigorítják: *"106. § (1) Aki a törvényben meghatározott eseteken kívül a szerzői jog tulajdonosának hozzájárulása nélkül a művet, adaptációját vagy átiratát másolja, forgalmazza vagy, nyilvánosságra hozza három évig terjedő szabadságvesztéssel is büntetendő.*
(2) A kísérlet is büntetendő."

Ha az elkövető kereskedelmi céllal kívánja forgalmazni a szerző művét engedély nélkül, úgy a *109. §* alapján akár 5 évig terjedő szabadságvesztéssel is sújtható.

Meghatározó a német Legfelsőbb Bíróság döntése az ún. "Inkasso" - ügyben, amelyben megállapítja, hogy csak az átlagos tudású programalkotó teljesítményét meghaladó alkotás tarthat igényt a szerzői jogi védelemre.[229]

Hazánkban az 1969. évi II. tv. végrehajtási rendeletének 1983-as módosításával kerül a szoftver a szerzői jog tárgyai közé. Az ET. (89) 9. sz. Ajánlásában a minimális listán szerepel a "védett számítógépes programok jogtalan reprodukálása" elnevezéssel összefoglalt kriminalizálni javasolt magatartások. E körbe tartoznak a jogi védelmet élvező számítógépes programok jogosulatlan másolása, forgalmazása vagy nyilvánosságra hozatala.[230]A fakultatív listán további tevékenységek büntetőjogi üldözését ajánlják. Ezen magatartások közé tartozik a számítógépes szoftverek szándékos, és vagyoni haszonszerzés végett történő másolása vagy használata. Az ET. Ajánlása a szoftver illegális másolásának, forgalmazásának és nyilvánosságra hozásának kriminalizálására koncentrál. Jóllehet a belső jogok nemcsak a szerzői jogsértés egy - egy elemét emelik ki, hanem a szerző személyhez fűződő és vagyoni jogainak teljességét védik. A jogosulatlan másolás és forgalmazás egyszerre sérti a szerző személyi és vagyoni jogait. A

---

[229] Moritz H-W - Thybusseck: Computersoftware. München, 1992. s. 40. (BGH. NJW. 1986.)
[230] CE Recommendation (89) 9. Appendix I. p(s). 105-106. és Csonka Péter: Council of Europe Activities Related to Information Technology .... id. mű p. 184.

szerzői jog büntetőjogi védelmének kialakításának kérdése a kilencvenes évek elején kerül napirendre. Erre így emlékezik **Bárd Károly**: "1990. nyarán, amikor leginkább a nemzetközi szervezetek részéről az első noszogatások érkeztek, a büntetőjog nagy visszavonulásának bűvöletében elő jogszabály-előkészítő stáb még ellenállt, majd mintegy kompromisszumos megoldásként kriminalizálták a szándékos elkövetést. És nem biztos, hogy a végsőkig fogunk harcolni álláspontunk mellett, ha a parlamenti vitában a gondatlan elkövetés büntetését is indítványozni fogják."[231] Ugyanakkor a számítógépes szoftverek civiljogi védelméről 1991-ben az Európai Közösségek Tanács 91/250. sz. irányelvében kijelöli a megteendő intézkedések kereteit. (Bizonyos módosítást eredményez a Tanács 1993-ban kelt 93/98-as irányelve.)[232] A magyar Btk. 1993-as módosítást megelőzően a szerzői jogsértés egy szegmensére koncentrálnak, és társítják tipikus kriminális elemekkel. A bitorlás tényállását valósítja meg az, aki más szellemi alkotást sajátjaként tünteti fel, és ezzel vagyoni hátrányt okoz, vagy szellemi alkotásból származó haszonból részesedést követel. A szerzői és szomszédos jogok megsértése a kriminalizálásáig a 17/1968. (IV. 14.) Kormány számú rendelet 165. §-ban meghatározott szabálysértésnek minősül.

A **magyar** büntető törvénykönyv 1993. évi XVII. törvénnyel a szerzői jog már ismert civiljogi védelmét erősítik. A törvényhely legutóbbi módosítása 1999-ben történik.

"329/A. § (1) Aki irodalmi, tudományos vagy művészeti alkotás szerzőjének, művén, előadóművésznek előadói teljesítményén, hangfelvétel előállítójának hangfelvételén, rádió- vagy televízió-szervezetnek a műsorán, illetőleg film előállítójának a teljesítményén fennálló jogát haszonszerzés végett vagy vagyoni hátrányt okozva

---

[231] Dr. Bárd Károly: A büntetőjogi kódifikáció kérdései. Kriminológiai Közlemények 47. kötet. Budapest, 1993. 104.l.

[232] EK. Hivatalos Lap L.122/44. 1991.5. szám 42.l. és angol nyelven: Official Journal of the European Communities No. L.122/44. 17.5.91.

megsérti, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) A büntetés bűntett miatt három évig terjedő szabadságvesztés,

ha a szerzői és szomszédos jogok megsértését

a./ jelentős vagyoni hátrányt okozva,

b./ üzletszerűen követik el.

(3) A büntetés

a./ öt évig terjedő szabadságvesztés, ha a szerzői és szomszédos jogok megsértését különösen nagy vagyoni hátrányt okozva követik el,

b./ két évtől nyolc évig terjedő szabadságvesztés, ha a szerzői vagy szomszédos jogok megsértését különösen jelentős vagyoni hátrányt okozva követik el.

(4) Aki a szerzői és szomszédos jogok megsértését vagyoni hátrányt okozva gondatlanságból követi el, vétség miatt egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő."

A bűncselekmény tevékenységi tárgyai között szerepel a számítógépes szoftver is. Az Szjt. védi a "számítógépi programalkotás és a hozzá tartozó dokumentáció (a továbbiakban: szoftver) akár forráskódban, akár tárgykódban vagy bármilyen más formában rögzített minden fajtája, ideértve a felhasználói programot és az operációs rendszert is" (1. § (1) bekezdés c. pontja). A szoftver már a *fejlesztés fázisában* is büntetőjogi védelmet kap. Az LB. egyik eseti döntése megállapítja, hogy a számítógépes programfejlesztő folyamat egyes elkülöníthető szakaszai is létrehozhatnak olyan önálló alkotásokat, amelyek külön szerzői jogi oltalomban részesülhetnek.[233] **Bércesi Zoltán** a program eredetisége kapcsán megjegyzi, hogy "a számítógépi programra vonatkozó ötlet alkotó megvalósítása nem másodlagos mű, még akkor sem, ha voltaképp az ötletgazda gondolatának "feldolgozása",

[233] BH 1993. 545.sz

hanem eredeti software-alkotás".[234] A szerzői jog védelme kiterjed arra a szoftverre is, amelyet az eredetiről *eltérő programnyelvre* írtak át (Szjt. 58. § (2) bekezdés). A számítógépes *adattár* szerzői jogi védelme egyelőre nem komform az Európai Unió idevágó normájával. A Szjt. 7. § (3) bekezdése szerint "a gyűjteményes műnek minősülő - számítástechnika eszközökkel vagy bármely más működtetett - adattár védelme nem terjed ki a tartalmát képező adatokra és egyéb alkotóelemekre." Ezzel szemben a (96) 9. Európai Unió (EU) (III. 1.) Tanácsának Irányelve javasolja, hogy ne csak az adatbázis elrendezése, egyéni rendszere élvezzen jogi védelmet, hanem az adatbázis tartalmi része. Ez a rendezés tenné lehetővé azt, hogy az adatbázis létrehozója élni tudjon engedélyezési jogával az adatbázisi egészének vagy bármely részének felhasználását illetően.[235]A kormányzat jogharmonizációs programja 2001-re ígéri ezen ellentmondás feloldását.

A bűncselekmény elkövetési magatartása a szerzői jog - amelyben "a személyhez fűződő és a vagyoni elemek egymással összefonódnak"[236]- megsértése. A szerzőt eme jogösszesség a mű létrejöttétől kezdve megilleti (Szjt. 9. § (1) bekezdés). Ezt a keretdiszpozíciót az 1999. évi LXXVI. tv. pozitív rendelkezései töltik ki. Tehát akár a szerző személyhez fűződő, akár vagyoni jogosultsága sérül, és ezzel összefüggésben vagyoni hátrányt szenved, akkor megindítható a büntető eljárás. A bűncselekmény - hasonlóan a számítógépes csaláshoz - haszonszerzés céljából, részben károkozási szándékkal valósítható meg.

A szerző személyhez fűződő jogai különösen:

- művének nyilvánosságra hozataláról való döntés (Szjt. 10. § (1) bekezdés),

---

[234] Dr. Bércesi Zoltán: A szerzői jogi jogharmonizáció az Európai Közösségben, a computer - software termékek védelméről szóló irányelv hatásai a magyar szerzői jogban.

MJ. 42. 1995. 7. 397-398.l.

[235] Az 1999. évi LXXVI. törvény 1. § (3) bekezdéséhez fűzött Indokolás. Megjelent: a CompLex Jogtárban.

[236] Dr. Gyertyánfy Péter: A szerzőség fogalma és a mű hasznosítására kötött szerződések. MJ. 1994. 11. 642.l.

- szerzői minőségének elismerése (Szjt. 12. § (1) bekezdés), ideértve az át- vagy feldolgozást, fordítást stb. (Szjt. 12. § (2) bekezdés),
- művének integritásához való jog (Szjt. 13. §),
- művének visszavonásának a joga (Szjt. 11. §) stb.

Ezen jogok időben korlátlanok, azokról nem mondhat le, főszabályként másra át nem ruházhatja, kivéve ha felhasználási szerződésben a felhasználót erre felhatalmazza (Szjt. 15. §).

A szerző vagyoni jogai különösen:

- a szerző hozzájárulása a mű felhasználásához, (Szjt. 13. § (1) bekezdés),
- művének felhasználása során díjazás illeti meg, (Szjt. 16. § (4) bekezdés) stb.
- a szerző kizárólagos joga művének többszörözése, vagy erre engedély adása (Szjt. 18. § (1) bekezdés).

Többszörözésként értékelhető:

a. a mű anyagi hordozón való - közvetlen vagy közvetett - rögzítése, bármilyen módon, akár véglegesen, akár időlegesen, valamint

b. *b.* egy vagy több másolat készítése a rögzítésről (Szjt. 18. § (1) bekezdés a./ és b./ pontjai).

A technikai eszközök fejlődése, sokféleségük folytán a művek másolásának megoldásai is eltérőek. Az Szjt. megpróbálja egy csokorba kötni a legkülönfélébb többszörözési technikákat: "A mű többszörözésének minősül különösen a nyomtatással megvalósuló mechanikai, filmes vagy mágneses rögzítés és másolatkészítés, a hang- vagy képfelvétel előállítása, a sugárzás vagy a vezeték útján a nyilvánossághoz történő közvetítés céljára való rögzítés, *a mű tárolása digitális formában elektronikus eszközön, valamint a számítógépes hálózaton átvitt művek anyagi formában való előállítása.....*" (Szjt. 18. § (2) bekezdés). **Gyertyánfy Péter** idézi az osztrák Legfelsőbb Bíróság digitális adatátvitelre vonatkozó ítéletét, amelyben kimondja, hogy a file-transfer egyszerre jelent többszörözést és

terjesztést, vagyis ezek engedélykötelesek.[237] A szerző vagyoni jogai nem ruházhatók át, másként sem szállhatnak át és azokról lemondani sem lehet (Szjt. 9. § (3) bekezdés). Ezen rendelkezések alól az öröklés lehetősége jelent kivételt (Szjt. 9. § (4)-(5) bekezdés).

A Btk. 329/A. § alkalmazására általában akkor kerül sor, amikor a szerzői művet *jogosulatlanul felhasználják.* Az új Szjt. immár részletezi a jogosulatlan felhasználás tipikus eseteit, tehát

a. az engedély nélküli felhasználás vagy

b. a felhasználói jogosultság határainak túllépése (Szjt. 16. § (6) bekezdés).

Ad a. Engedély nélküli a szerzői mű felhasználása akkor, ha azt jogszabályi (pl. szabad felhasználás) illetőleg a szerző hozzájárulása nélkül történik.

Ad b. A felhasználói jogosultság határainak túllépése pl. a példányszám vagy egyéb területi, időbeli korlát túllépése.

Ha e jogok sérülnek és ezzel okozati összefüggésben a szerzőt - jelenleg - 2 millió forintig terjedő vagyoni hátrány éri, úgy a bűncselekmény alapesete valósul meg. A minősített esetek az elkövető által okozott vagyoni hátrány mértékéhez igazodnak.

A (2) bekezdés bűntetté nyilvánítja azt az esetet, amikor a szerzői jog megsértése jelentős vagyon hátrányt okoz, vagy a bűncselekményt üzletszerűen követik el. A jelentős vagyoni hátrány 2 és 50 millió forint közötti összeg. Üzletszerűen követi el a cselekményt az, aki rendszeres haszonszerzésre törekszik tevékenységével. Megjegyzendő, ahogy már fentebb utaltam rá, nem szükséges, hogy az elkövető több ilyen magatartást tanúsítson. Elegendő egyetlen cselekmény is, ha ezzel összefüggésben bizonyítható a rendszeres haszonszerzésre való törekvés.

A (3) bekezdés a. pontjában meghatározott különösen nagy vagyoni hátrány az 50 millió forintot meghaladó, de az 500 millió forinton belül maradó összeg, míg

---

[237] idézi az 1999. évi LXXVI. törvény 18. § (1) bekezdéséhez fűzött Indokolás Dr. Gyertyánfy Péter: Internet és a szerzői jog. c. tanulmányát. Megjelent: a CompLex Jogtárban.

a b. pontban szereplő különösen jelentős vagyoni hátrány az 500 millió forintot meghaladó összeg értendő.

A vagyoni hátrány megállapításához elsődleges szempont a sértett erre vonatkozó állítása, más esetben a felhasználási szerződés rendelkezései lehetnek iránymutatóak. Gyakorta kerül sor szakértő igénybevételére.

Vagyoni hátrány a büntetőjogban a polgári jogban ismert kár fogalommal esik egybe: így a vagyonban bekövetkezett értékcsökkenés mellett számításba kell venni az elmaradt hasznot is.

A szoftver illegális telepítésével a bűncselekmény befejezetté válik. Ám ennek további felhasználása nem büntetlen utócselekmény, hiszen a szoftver futtatása a vagyoni hátrányt növeli. Azt is mondhatjuk, hogy a bűncselekmény a szoftver további használatával állapot-bűncselekménnyé válik. így az elévülés is csak a szoftver utolsó futtatásától kezdődik.

A törvény büntetni rendeli a gondatlan elkövetést is, rendkívül megszigorítva a büntetőjogi fellépés lehetőségét. A szerzői jogok megsértése bűncselekményének a rendbeliségét a megsértett szerzői jogok száma, általában tehát a sértettek száma határozza meg.

Mivel az Szjt. vadonatúj, így alkalmazásának esetleges nehézségei még nem válhatnak ismertté. A szerzői és szomszédos jogok büntetőjogi védelme - véleményem szerint - túlkriminalizált. Ma általában az otthoni számítógépeken felbecsülhetetlen számú illegális forrásból szoftver fut. Ezen programokat elsősorban a fiatalabb korosztály használja. Több tíz- vagy százezer számítógép - lehetőleg időben egyszerre történő - ellenőrzése a törvény betartása végett *lehetetlen*. A Btk. e félresikerült rendelkezése potenciális bűnelkövetőket kreált. Tudomásul kell venni, hogy életünk más negatív jelenségéhez hasonlóan a szoftvermásolás, a nem regisztrált programok alkalmazása, másolása, cserélgetése sem tiltható meg büntetőjogi szigorral. A szoftverek illegális használatának abbahagyásáért és az ebből eredő, igazolt vagyoni kár érvényesítéséért a polgári peres eljárás tág lehetőséget nyit. *A büntetőjog - nem győzzük hangsúlyozni - "ultima ratio" a jogi felelősség érvényesítésében.* Előtérbe tolása szereptévesztés, és

a gyengeség jele. E realitást a jogtulajdonos lobbynak is el kell fogadnia. (Egyébiránt a szoftvergyártók sem mindig "fehér bárányok". Gondoljunk arra az esetre, amikor a WordPerfect cég 1990-ben vírusfertőzött programot hoz forgalomba Ausztráliában[238], vagy a Microsoft cég perére, amelyben a híres szoftvergyártó cég tisztességtelen piaci magatartások sorával teszi tönkre a konkurenciát.)[239]Megfontolandó az extraprofittal "terhelt" irreálisan magas szoftver árak fenntartása, hisz döntően ez indukálja a szoftverek tiltott másolását. Árcsökkentéssel, az ügyféli kör kialakításáért, majd megtartásáért ár- és egyéb piaci kedvezmények alkalmazásával, az illegális szoftverhasználóval mindkét fél számára előnyt kínáló megegyezéssel, végül polgári bíróság előtt érvényesített kártérítési perben véleményem szerint hatékonyabban biztosíthatók a szerzői jogok. Sem mint túlkriminalizált és betarthatatlan büntetőjogi szabályok belobbizásával.

A *büntetőjogi szigornak* a szoftverek üzletszerű másolóival és kereskedőivel szemben kell érvényesülnie. Ők sértik igazán a jogtulajdonosok vagyoni és piaci érdekeit. A küzdelmet e területre kell koncentrálni.

Ezen túlmenően a jogi szabályozás kapcsán az Interneten megjelenő, illetőleg azon keresztül elérhető szerzői művek jogi védelme vet fel aggályokat. Ugyanis e művek lehívhatók, rögzíthetők, többszörözhetők, ezáltal teljességgel kikerülnek a szerző vagy jogszerű felhasználó ellenőrzése alól. A hazai polgári bíróságok gyakorlata fog utat nyitni az Interneten elérhető művek szerzői jogi problémáinak megnyugtató megoldásához.

6. 11. A védett mikroeletronikai félvezetők jogosulatlan másolása, kereskedelme

A hatvanas években az amerikai *Bob Noyce* egy kicsiny szilikondarabra elektromos áramköröket tömörített, és ezzel a számítástechnika fejlődését meggyorsította. Az első szabadon programozható chipet az Intel cég mutatja be

---

[238] Kis János - Szegedi Imre ..... id. mű 32.l.

[239] internetto.hu/rovat/e-vilag/szoftver/ C0002362.htm

1971-ben.[240] Ez még 2300 tranzisztort tartalmazza (mellesleg ekkora számítási kapacitással bírt az 1946-ban készült ENIAC). Az első bemutatott chip 4 bitnyi információt tartalmaz. Ezután jönnek a 8 bites 8008-as, majd a 16 bites 8086-as és a 8088-as chipek. A 286-os számítógépek 134 ezer tranzisztort, míg a 386-os gépbe annak duplája, a 486-os gépbe annak tízszerese került Napjainkban a Pentium I. Pro 5,5 millió tranzisztorral rendelkezik, és már általánossá a Pentium II., és itt van a Pentium III.[241]

Míg a félvezetők fejlesztéséhez, hasonlóan a szoftver előállításához jelentős összegű technikai-, technológiai, financiális, sőt munkaerő invesztíció szükséges, amely felöleli a műszaki fejlesztés, a nem olcsó (pl. steril) gyártási környezet kialakítást, majd a marketing költségeit. Nyilvánvalóan nem véletlen, hogy a konkurenciát legyűrni szándékozó ipari kémek kiterjesztik figyelmüket, sőt a szervezett bűnözők is megjelennek. Meghökkentő és egyben figyelmet felkeltő annak az angol bandának a ténykedése, amely a British Telecommunications egyik számítógépközpontjába betörve, a cég számítógépeiben levő chipeket kilopta. Nem hiszem, hogy kétséges az, a bűnbanda megrendelésre dolgozott.[242] Hiszen pl. a lopott chipek, de ugyanígy merevlemezek, és a mikroprocesszorok felvevő piaca bőséges, busás hasznot ígér. Kezdve hazai és külföldi szervizeiktől, a rendszerek korszerűsítésére szakosodott szervezeteken át távoli országok illegális (netán legális?) összeszerelő üzeméig. Az ilyen bűncselekményeket lehetővé tevő ok az, hogy a régebbi számítógépekben a chipek sorszám nélkül készülnek és kerülnek a gépekbe. Talán napjainkban erre is nagyobb figyelem összpontosul. Ugyanakkor a félvezetők mintázata érték. Egy - egy parányi szilíciumlapocskán elhelyezett áramkörök elrendezése jelenti, hogy milyen feladatot, és mennyi idő alatt stb. képes elvégezni a chip. Éppen ennek fontossága és persze gyártásuk költségessége kész-tette a jogászokat arra, hogy a félvezetők jogi védelmének feltételeit megteremtsék.

---

[240] www.intel.com/intel/museum/25anniv/iwh/iwhq2a.htm

[241] Csajbók Zoltán id. mű .... 42 - 54.l.

[242] adja hírül a Népszabadság 1995. szeptember 26. 14.l.

A vita akkor azon zajlik, hogy hol helyezhetők el e termékek. A szabadalomra vonatkozó jogi védelem adoptálható, mivel a nyomtatott áramkör előállítása is ismert, szabadalmaztatott eljáráson alapult és a chip értékét annak mintázata jelenti.Ezért *sui generis* jogi oltalom megteremtése felé tolódik el a hangsúly. Speciális jogi formát alkotnak egyes országok adoptálva a már ismert civil- és más jogi eszközöket. Az Egyesült Államok lép először, és 1984-ban megalkotja "A félvezetők védelméről" szóló törvényt, példáját nemsokára Japán követi, amely 1985-ben hirdeti ki törvényét. Kontinensünkön az Európa Közösség 1986. december 16-án kelt Ajánlásában javasol a félvezetők jogi védelmének kialakítását az egyes országokban. Hollandiában 1987-ben születik meg a chipvédelmi törvény.

Az **ET. (89) 9. sz. Ajánlás** a mikroelektronikai félvezetők büntetőjogi védelmének kialakítására vonatkozóan az alábbi magatartásokat javasolja tilalmazni: a védett topográfiákról jogtalan másolat készítése, félvezető termékek készítése, kereskedelmi forgalmazása vagy behozatal végett, továbbá ezek felhasználása dokumentációk vagy gyártmányok előállítása céljából.[243]

A **magyar** törvényhozás 1991-ben hozza meg "A mikroelektronikai félvezető termékek topográfiájának oltalmáról" szóló törvényt. Ebben azt olvashatjuk, hogy:

"1. § (2) A topográfia a mikroelektronikai félvezető termék elemeinek, amelyek közül legalább egy aktív elem, és összeköttetéseinek vagy azok egy részének bármely formában kifejezett, térbeli elrendezése vagy egy gyártásra szánt félvezető termékhez készített ilyen térbeli elrendezés.

(3) A topográfia eredeti, ha az saját szellemi alkotómunka eredménye és megalkotása idején nem szokásos az iparban.

(4) A szokásos részekből álló topográfia oltalmazható, ha azok elrendezése eredeti."

---

[243] CE Recommendation (89) 9. Appendix I., és Csonka Péter: Council of Europe Activities Related to Information Technology .... id. mű p. 184.

E szakasz további bekezdéseiben részben pontosítja, részben kiterjeszti a topográfia fogalmát. A félvezetők topográfiájának jogi védelme jelenleg a polgári jogra korlátozódik, tehát polgári bíróság előtt érvényesítendő a károsult igénye. A félvezetők védelmének büntetőjogi megerősítése az 1999:CXX. törvénnyel valósul meg. A Btk. az alábbi 329/D. §-szal egészül ki:

(1) Aki a jogosultnak szabadalmi oltalom, használati vagy ipari oltalom, ***topográfiaoltalom****, védjegy vagy földrajzi árujelző oltalma alapján fennálló jogát az oltalom tárgyának utánzásával vagy átvételével megsérti, és ezzel vagyoni hátrányt okoz, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.*

(2) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha az iparjogvédelmi jogok megsértését

a./ jelentős vagyoni hátrányt okozva,

b./ üzletszerűen követik el.

(3) A büntetés

a./ öt évig terjedő szabadságvesztés, ha az iparjogvédelmi jogok megsértését különösen nagy vagyoni hátrányt,

b./ két évtől nyolc évig terjedő szabadságvesztés, ha az iparjogvédelmi jogok megsértését különösen jelentős vagyoni hátrányt okozva követik el."

Úgy vélem, hogy a félvezetők topográfiájának jogosulatlan megszerzése (lefényképezése vagy tervrajzának jogosulatlan elsajátítása stb.), amennyiben ez titok tárgyát képezi (pl. a tervező asztalon), úgy szolgálati titoksértésként értékelendő (Btk. 222. §-a.).

Viszont aggályos lehet büntetőjogi felelősséget érvényesíteni akkor, amikor az elkövető kereskedelmi forgalomból szerzi be a számítógépet, majd a félvezetőt kiszerelve azt másolja, forgalmazza stb. Az ET. ajánlásával összhangban megfontolandó a félvezetők büntetőjogi feltételeinek bővítése a félvezetők utánzása és átvétele mellett annak jogosulatlan felhasználásának, forgalombahozatalának a tilalmazása. De lege ferenda e magatartások előtérbe helyezésével keretdiszpozíció

lenne, amely struktúrájában a szerzői és szomszédos jogok megsértésének bűncselekményéhez hasonlítana.

6. 12. Bűncselekmények a hálózatokon, a nagy nyilvánosság előtt

A számítógépes hálózatok elterjedésével egyre gyorsabban, egyre nagyobb tömegű információ továbbítása, elérése vált valóra. Az Interneten, amelyet a katonák után tudósok, egyetemisták használtak először a kölcsönös bizalom légköre uralkodik. Nem volt szükség biztonsági intézkedésekre. A "régi szép időkben" megszerkesztett műszaki megoldások, szabványok teszik lehetővé ma a világháló sebezhetőségét. A világháló által elérhető adatállományok tartalmukban nemcsak hasznos vagy érdekes tudnivalókat közölnek, hanem sérthetik mások nyugalmát, jó ízlését.

A német **E. Hilgendorf** a hálón véghez vitt támadásokat tipizálva - **Opplinger** felosztását fejlesztve - különbséget tesz passzív és aktív jogsértések között:

- passzív támadás: az információk lehallgatása, az adatáramlás irányának, sűrűségének elemzése, kapcsolatok kifürkészése stb.
- aktív támadás: a behatoló beléphet védett adatállományokba és ott különböző jogsértéseket követhet el, továbbá a korábbi üzenetek (e-mail küldése, áru- vagy szolgáltatás rendelése) a feladó avagy címzett tudta nélkül újra küldhetők stb.[244]

A görög **Irini Vassiliki** a hálózati bűncselekményeket a jogellenes információk terjesztésére, illetőleg harmadik személy információs jogának sértésére osztja fel.[245]

Az egyesült államokbeli **Cole Durham** az alábbi jogsértő magatartások között különböztet:

- engedély nélküli hozzáférés az Internethez,
- kárt okozó tevékenység vagy kárt okozó anyagok közzététele,

---

[244] Dr. Erich Hilgendorf: Grundfälle zum Computerstrafrecht. JUS 1997.4. s. 323.
[245] I. Vassiliki id. mű (89. számon) ..... s. 298.

- információ illetéktelen elfogása.[246]

A szintén egyesült államokbeli **Olivier Hance** tipizálása felidézi az informatikai bűncselekmények kapcsán adódó dilemmát. Szerinte az Interneten elkövethetők:

- hagyományos bűncselekmények, amelyekhez az Internet kommunikációs eszközül szolgál (nem számítógépes bűncselekmények),
- magát a hálózatot és a számítástechnikai eszközöket használják fel bűncselekmények elkövetésére (számítógépes bűncselekmények).[247]

Napjaink realitása az, hogy korlátlanul közzétehetők, küldhetők szélsőséges politikai felhívások, gyűlöletkeltésére alkalmas, valamint durva pornográf képek, szövegek, ábrák, a drogfogyasztást népszerűsítő felhívások. De fellelhetők bombakészítés titkait felfedő ábrák, maffia - hirdetések, tilalmazott szövegek, könyvek, dalszövegek. Vagyis sok esetben a legálisan másutt fórumhoz nem jutó személyek, szervezetek jelenítik meg irományaikat, képeiket, dalaikat stb.

A *szabadság és a szabadosság információi* érhetők el és áramlanak milliószámra a világhálón. Korántsem véletlen az, hogy egyes országok tiltják az Internetes kapcsolat kiépítését (pl. Azerbajdzsán, Kazahsztán)

A helyzet rendkívül *paradox*. Az adatbevitelt egy országban lehet tilalmazni, kriminalizálni, ám az adatok elérésének jogi tiltása megoldhatatlan. Amíg *valamennyi ország nem tilalmazza* a köznyugalmat és a jó ízlést sértő szövegek, ábrák bevitelét a hálózatokba, addig a büntetőjogi fellépés valójában hatástalan. Ha ilyen szövegek, képek, ábrák küldhetők bármely olyan országból, ahol ez nem büntetendő (eltérő erkölcsi felfogás folytán, netán a szólásszabadság jelszavával vagy ennek álcázott üzleti érdekből), akkor ezek az állományok elvileg elérhetők maradnak és a "tiltott gyümölcs" rendkívül piacképes. Megakadályozni vagy nehezíteni az ilyen adatállományok, programok elérését csupán technikai megoldásokkal lehetséges és tűnik szükségesnek.

---

[246] Cole Durham: Les structures émergentes du droit criminal de l'information: tracer les contours d'un nouveau paradigma. Revue Internationale de droit penal. Vol. 63. s. 1371.

A hálózatokban elkövethető bűncselekmények *általában nem* új típusú deliktumok, hanem a már ismert és a magyar Btk.-ban is kriminalizált magatartások. Tipikusan olyan bűncselekmények ezek, amelyek írásban, képnek, ábrának vagy rajznak a megjelenítésével követhetők el. Ez a szöveges, képes közlés kerül fel a hálózatokra, pontosabban azon adatállományokba, amelyek a hálózaton keresztül elérhető. E sommás állítás alól kivétel az elektronikus üzenetek titkosságát megtörő lehallgatás.

Még egy a cselekmények büntetőjogi értékelést befolyásoló kérdést kell tisztáznom. A bűncselekmény elkövetése az Interneten nagy nyilvánosság előtt történő elkövetésnek minősül az 1999. CXX. törvény óta. A Btk. értelmező rendelkezése szerint *"nagy nyilvánosságon a bűncselekménynek sajtó, egyéb tömegtájékoztatási eszköz, sokszorosítás, illetőleg elektronikusan rögzített információ távközlő hálózaton való közzététele útján elkövetését is érteni kell" (137. § 12. pont).*

Korábban az ítélkezési gyakorlatban a nagy nyilvánosság előtt történt elkövetés megállapításának a feltétele, hogy a bűncselekmény megvalósításakor nagyobb létszámú személy legyen jelen vagy *fennálljon annak reális lehetősége, hogy arról vagy annak eredményéről nagyobb, előre meg nem határozható és egyszeri ránézéssel meg nem számolható több személy szerezzen tudomást.*[248] Ez utóbbi feltételnek a számítógépes hálózatok mindenben megfelelnek, tehát indokolt a törvény kiterjesztő értelmezése.

Az Internetet és más hálózatokat nemcsak e szolgáltatásra előfizető magánszemélyek, hanem intézményekben, vállalatoknál dolgozók, tanulók is hozzá férhetnek. Ebből adódóan, ha a bűncselekmény hálózatokban valósul meg, úgy nagy nyilvánosság előtt elkövetettnek kell majd értékelnünk. Megfordítva e tételt, ha a nagy nyilvánosság előtt történő elkövetés a bűncselekmény *alapesete*, úgy a magatartás e speciális helyszínen megvalósulva minősül bűncselekménynek. Ha a nagy nyilvánosság előtt történő elkövetés a tényállás *minősített esete*, akkor a

---

[247] Olivier Hance: Üzlet és jog az Interneten. Budapest, 1977. 162-163.l.
[248] BJD. 9103

bűncselekmény súlyosabban büntetés kiszabásának lehetőségét vonja maga után. Ha a nagy nyilvánosság előtt történő elkövetés nem eleme a felhívott tényállásnak, úgy - véleményem szerint - a hálózatokon való véghezvitel súlyosító körülményként jön(ne) szóba.

Mindezek előrebocsátását követően lássunk *néhány* a számítógépes hálózatokon keresztül elkövethető bűncselekményt és azok *legalapvetőbb* jellemzőit:

A. Az emberi becsületet- és méltóságot sértő bűncselekmények

Az emberi becsület- és méltóság a személyiségi jogok elidegeníthetetlen része. Érvényesülése az emberi jogok biztosításának elsődlegességében ragadható meg. Az emberi becsületet- és méltóságot sértő cselekmények relatív állandósággal jelen vannak a jog, a büntetőjog rendszerében.

A büntető-jogtudomány klasszikusai a büntetőjogi védelem alá helyezett becsület fogalmára tett meghatározásokat **Angyal Pál** rendszerezi. Összegzése alapján az egyik nézet szerint "*a becsület az az érték, mellyel az emberi mivoltánál fogva és illetőleg erkölcsös és jogszerű viselkedése következtében bír* (Binding, Kohler, Finger), a másik nézet viszont nem erre az általános emberi méltóságra, nem az erkölcsi, hanem a társadalmi értékre helyezi a súlyt s azt vitatja, hogy *a becsület az embernek az a szociális értéke, melyet sajátos társadalmi kötelességeinek teljesítésére szükséges tulajdonságok birtoka és azoknak megfelelő cselekvése útján szerez meg* (Liszt, Liepmann, Frank)."[249]

Finkey Ferenc úgy véli, hogy a becsület fogalma két jogi értéket ölel fel, egyfelől az egyénnek általános *emberi méltóságát*, másfelől az egyén *személyes erkölcsi értékét*.[250]

---

[249] Dr. Angyal Pál: A magyar büntetőjog tankönyve. Második kötet. (Különös rész. 2. füzet) Budapest, 1918. 264.l.

[250] Dr. Finkey Ferenc: A magyar büntetőjog tankönyve (26., 57., 154. számokon)

.....

Ma az általánosan elfogadott vélemény szerint a becsület az emberről, magatartásáról, tulajdonságáról, egyéb emberi értékéről a társadalmi környezetében kialakult kedvező ítélet. Az emberi méltóság az adott személy egyéni önértékelésének tiszteletben tartását jelenti.

A **magyar** büntető kódexben két egymással összefüggő tényállás védelmezi a becsület kétoldalát, amely azonban nem fedi le egymást szükségképpen.

Rágalmazás

"179. § (1) Aki valakiről, más előtt, a becsület csorbítására alkalmas tényt állít vagy híresztel vagy ilyen tényre közvetlenül utaló kifejezést használ, vétséget követ el, és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) A büntetés két évig terjedő szabadságvesztés, ha a rágalmazást

a./ aljas indokból vagy célból,

b./ nagy nyilvánosság előtt,

c./ jelentős érdeksérelmet okozva követik el."

Számítógépes környezetben ez a bűncselekmény akkor állapítható meg, ha a hálózatra felkerült becsületsértő adatállomány (szöveg, kép, rajz, hang-file stb.) tényközlés vagy tényre közvetlenül utal. Tény jogi értelemben: a múltban és jelenben megtörtént emberi magatartások, események, jelenségek, történések, a szubjektív tudatállapot létezése. A jövőre utaló tényközlés a becsületsértés körébe tartozik.

A bűncselekmény sértettje csak határozottan felismerhető, személyében azonosítható, élő személynek kell lennie. Gyermekek vagy kóros elmeállapotú személy ugyanúgy lehet passzív alany, mint jogi személy. A tényközléssel vagy az erre közvetlenül történő utalással megvalósuló becsületsértés megítélése nem a sértett szubjektív értékítélete, egyéni megítélése, érzelmi beállítottsága vagy érzékenysége alapján kell megítélni, hanem azt kell vizsgálni, hogy a tényállítás

---

id. mű 664.l.

objektív értelmezés alapján és a társadalomban kialakult általános felfogás szerint alkalmas-e a becsület csorbítására.[251]

A becsületsértő tények vagy tényre történő utalások megjelenítése, elérhetősége valamely hálózaton a rágalmazás minősített esetének megállapítására ad alapot. Ha az elkövető valótlan tényközlésben a sértettnek tulajdonít valamely bűncselekmény, szabálysértés vagy fegyelmi vétségnek minősülő magatartás megvalósítását *és* ezt a hatóságnak e-mail-en küldi el, akkor ez megfelel a Btk. 233. §-ban szabályozott *hamis vád* bűncselekményének. De nem ez a tipikus elkövetési helye a hamisan vádolásnak, ám a jövőben erre számítani lehet.

Ha az elkövető a sértett emberi méltóságát gyalázkodó tartalmú adatközléssel valósítja meg, vagy bár tényközlés történik, de ezt közvetlenül a sértettnek e-mail-en keresztül küldi meg, akkor - a becsületsértés szubszidiaritása miatt - ez utóbbi szerint minősül.

Becsületsértés

"180. § (1) Aki a 179. § esetén kívül mással szemben

a./ a sértett munkakörének ellátásával, közmegbízatásának teljesítésével vagy közérdekű tevékenységével összefüggésben,

b./ nagy nyilvánosság előtta becsületcsorbítására alkalmas kifejezést használ vagy egyéb ilyen cselekményt követ el, vétség miatt egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő, aki a becsületsértést tettlegesen követi el."

Számítógépes hálózatokon a becsületsértés bűncselekménye a tény- vagy a tényre utaló közlésen kívül minden más, általában gyalázkodó, becsmérlő, megszégyenítő stb. írással, képábrázolással, hanganyag elérhetőségével, közzétételével megvalósítható, amely az emberi méltóság megsértésére alkalmas. Általában az egyszerű illetlenség, trágárság, gúnyolódás nem elégséges feltétel a becsületsértés megállapításához. Ha a becsületsértést nem a sértett munkakörének ellátásával, közmegbízatásának teljesítésével illetve közérdekű tevékenységével összefüggésben követik el, akkor a becsületsértés szabálysértése állapítható meg.

---

[251] BJD. 8970., továbbá BH. 1992/226. sz. és 1994/171. sz.

Ha a hálózaton elérhető információ, képábrázolás nem élő személy, hanem elhalt becsületét sérti, akkor a Btk. 181. § *kegyeletsértés* bűncselekménye állapítható meg. Ebben a tényállásban a "nagy nyilvánosság" nem tényállási elem. A hálózaton történő elkövetést a bíróság súlyosító körülményként veheti figyelembe.

B. A köznyugalmat sértő bűncselekmények:

1. A *közösség elleni izgatás*

"(1) Aki nagy nyilvánosság előtt

a./ a magyar nemzet,

b./ valamely nemzeti, etnikai, faji, vallási csoport vagy a lakosság egyes csoportjai ellen gyűlöletre uszít bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."

A törvényi tényállás tehát taxatíve felsorolja a bűncselekmény közvetlen tárgyait, amelyet a hálózaton elérhetők, vagy megjelenített szövegnek, képek, ábráknak, grafikának, esetleg konkludens tény megjelenítésével sérteniük kell. Ezen közléseknek alkalmasnak kell lenniük gyűlöletre történő uszításra, amely nem azonos az izgatás fogalmával. Míg ez utóbbit a tudatra történő hatásként definiálhatjuk, addig az uszítás legjellemzőbb sajátossága a durva érzelmi ráhatás más személy pszichikumára. A gyűlöletkeltére alkalmas cselekmény tartalmát tekintve nem más, mint hátrányos értékítélet, dehonesztáló vélemény megjelenítése e körben a számítógép lehetőségeivel. A gyűlöletkeltés dinamikáját tekintve nem más, mint a gyűlöletet kelteni kívánkozó személy gondolatainak közvetítése a védett jogtárgyak felé. A közösség elleni izgatás nem eredmény bűncselekmény, nem szükséges, hogy a gyűlölet az információkhoz jutó személyekben ténylegesen kialakuljon. A bűncselekmény befejezettségéhez elégséges ennek távoli veszélye is. A törvényi tényállás további tárgyi elemei között szerepel a "nagy nyilvánosság előtt" történő elkövetés. Ez a feltétel is adott a 2000.

március elsejétől hatályos Btk. módosítást követően. Ugyanakkor irreleváns az, hogy ezen információk milyen nyelven olvashatók a számítógépes hálózatban.

2. Amennyiben az adatállományok tartalma különféle jogi normákkal szemben történő engedetlenségre uszításra alkalmas, úgy a *"a törvény vagy hatósági rendelkezés elleni izgatás"* hívható fel: *"Aki nagy nyilvánosság előtt, a köznyugalom megzavarására alkalmas módon törvény vagy más jogszabály, avagy a hatóság rendelkezése ellen általános engedetlenségre uszít, bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő."*

Engedetlenség a jogszabályokban írt magatartás tanúsításának kétségbe vonását vagy ezekkel szemben passzív ellenállásra való felhívást jelenti. Ennek a köznyugalom megzavarására alkalmasnak kell lenni.

3. A *nemzeti jelkép megsértése*

"269/A. § Aki nagy nyilvánosság előtt a Magyar Köztársaság himnuszát, zászlaját vagy címerét sértő vagy lealacsonyító kifejezést használ vagy más ilyen cselekményt követ el, ha súlyosabb bűncselekmény nem valósul meg, vétség miatt egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő."

A bűncselekmény jogi tárgya Magyarország nemzeti jelképei, amelyeket az Alkotmány 75. és 76. §-ai határozzák meg. Minden olyan tartalmú írás-, hang vagy képközlés, amely a védett jelképeket lealacsonyítja vagy az ezekhez fűződő nemzeti érzést sérti. E lealacsonyító vagy sértő közlésnek közvetlenül a védett jelképekre kell vonatkozniuk és félreérthetetlennek kell lennie.

4. Az *önkényuralmi jelképek használata*

"269/B. § (1) Aki horogkeresztet, SS-jelvényt, nyilaskeresztet, sarló-kalapácsot, ötágú vöröscsillagot vagy ezeket ábrázoló jelképet

a) terjeszt;

b) nagy nyilvánosság előtt használ

c./ közszemlére tesz;

ha súlyosabb bűncselekmény nem valósul meg, vétséget követ el, és pénzbüntetéssel büntetendő.

(2) Nem büntethető az (1) bekezdésben meghatározott cselekmény miatt, aki az ismeretterjesztő, oktatási, tudományos, művészeti célból vagy a történelem, illetve a jelenkor eredményeiről szóló tájékoztatás céljából követi el.

(3) Az (1) - (2) bekezdés rendelkezései az államok hatályban levő hivatalos jelképeire nem vonatkoznak."

E jelképek a hatalom erőszakos megragadó, a hatalomgyakorlás diktatórikus módját megvalósító politikai pártokhoz, irányzatokhoz, személyekhez kötődő szimbólumai. Ezek terjesztése vagy megjelenítése a hálózatokban az állampolgárok jelentős részében félelmet, riadalmat, de legalább ellenérzést váltanak ki.

5. A *rémhírterjesztés.*

"270. § (1) Aki nagy nyilvánosság előtt olyan valótlan tényt - vagy való tényt oly módon elferdítve - állít vagy híresztel, amely alkalmas a köznyugalom megzavarására, vétséget követ el, és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.(2) a büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a rémhírterjesztést közveszély színhelyén vagy háború idején követik el."

Bevezetőben említem, hogy az Alkotmánybíróság várhatóan 2000. év nyarán dönt a rémhírterjesztés tényállása alkotmányosságáról.

A rémhírek hatása az, hogy az arról tudomást szerzőkben nyugtalanságot, súlyosabb esetben pánikot kelt. Ez a hatás a hálózatokban történő közléssel szintén elérhető. Ezen információk vagy valótlan tényeket vagy a valóságtól elferdített tényeket jelenítenek meg a különféle hálózatokon.

E bűncselekmény befejezettségéhez csupán annyi szükséges, hogy a köznyugalom megzavarásának lehetősége reálisan fennforogjon. A társadalom tagjaiban nyugtalanító hatást váltson ki, zavart, netán pánikot keltsen. Egy - egy

értelmező rendelkezés alkalmazása legfeljebb azért merülhet fel, hogy tudatosítsuk, "nevezzük nevén" a büntetőjogi védelem lehetőségét.

6. A *közveszéllyel fenyegetés*

„270/A. § (1) Aki más előtt olyan, a köznyugalom megzavarására alkalmas valótlan tényt állít, hogy közveszéllyel járó esemény bekövetkezése fenyeget, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha az (1) bekezdésben írt bűncselekményt radioaktív anyaggal fenyegetve követik el.

(3) A büntetés az (1) bekezdés esetén három évig, a (2) bekezdés esetén öt évig terjedő szabadságvesztés, ha a közveszéllyel fenyegetés a köznyugalmat súlyosan megzavarta."

Ez a tényállás a rémhírterjesztés azon speciális esetére vonatkozik, amikor az elkövető közveszéllyel járó esemény előidézésével fenyeget. A közveszély meghatározatlan számú személyeket vagy meghatározatlan számú anyagi javak veszélyét jelenti. Ez általában az előidézhető energia, illetve a tűz pusztító hatásának kiváltására való utalás. Ha a fenyegető radioaktív anyagok alkalmazását helyezi kilátásba, akkor a bűncselekmény minősített esetéért vonható felelősségre.

C. Gyermekpornográfia

A számítógépes hálózatba felvitt információk olyan szexuális cselekményeket írhatnak körül, ábrázolhatnak, amely alkalmas a társadalom tagjainak megbotránkoztatására. Nem problémamentes annak eldöntése, — tekintettel napjaink viszonylag szabadabb morális felfogására, a szélsőségbe hajló szexualitás toleránsabb kezelésére — hogy hol húzódik, hol húzható meg generaliter az a határ, amelynek átlépése már a társadalom tagjainak a szexualitásról vallott morális felfogását sérti. Különös tekintettel arra, hogy már most működnek vetkőző számokra specializált, előfizethető hálózatok, vagy az egyre merészebb társkereső szolgáltatások illetve az a tény, hogy erotikus újságok is megjelennek a

hálózatokban. Azonban durva pornográf, obszcén szövegek, a szexualitást lealacsonyító módon ábrázoló képek, ábrák, szövegek közlése a hálózatokban sértheti a társadalom értékítéletét, morális felfogását.

Rendkívül súlyos veszélyeket rejt a **gyermekpornográfia** megjelenése a világhálón. Felnőttek perverz vágyainak kiszolgáltatott kiskorúakról készült képek kerülnek forgalomba térítés fejében. Az 1999-ben Bécsbe összehívott "Küzdelem az Interneten elérhető gyermekpornográfia ellen" konferencia záródokumentumában megfogalmaz néhány a büntetőjogban, illetve a nemzetközi bűnügyi együttműködésben alapvető tételt: így a zéró tolerancia elvét e cselekményekkel szemben, globális együttműködés fontosságát a nemzeti és nemzetközi szervezetek, kormányok valamint az Internet ipar között, továbbá a *gyermekpornográfia kriminalizícióját világszerte* stb. [252]Hazánkban a "tiltott pornográf felvételek készítése" elnevezésű tényállás - bár nem tartalmaz utalást az Internetre - alkalmazható erre az esetre is. Ez a tényállás az 1990-es new yorki "Egyezmény a gyermekek jogairól" nemzetközi dokumentum aláírását, majd belső jogba emelését (1991. évi LXIV. törvény) követően kerül a Btk. Különös részébe 1997-ben.

"Tiltott pornográf felvételek készítése"

"195/A. § (1) Aki kiskorú személyről video-, film-, fénykép- vagy más módon előállított pornográf képfelvételt vagy képfelvételeket készít, ilyen képfelvételt forgalomba hoz, azzal kereskedik, illetőleg ilyen képfelvételt más számára hozzáférhetővé tesz, bűntettet követ el, és két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő, aki pornográf jellegű műsorban kiskorú személyt szerepeltet.

(3) Két évtől nyolc évig terjedő szabadságvesztéssel büntetendő, aki az (1) - (2) bekezdésben írt bűncselekmény elkövetéséhez anyagi eszközöket szolgáltat.

---

[252] International Conference Combating Child Pornography on the Internet - Combating Child Pornography on the Internet - Conclusions and Recommendations. Ld.: www.stop-childporno.ag/conc_major.asp

(4) Az (1) - (2) bekezdés vonatkozásában pornográf képfelvétel, illetve pornográf jellegű műsor a nemiséget súlyosan, szeméremsértő nyíltsággal ábrázoló, célzatosan a nemi vágy felkeltésére irányuló, cselekvés, ábrázolás."

A bűncselekmény a kiskorú veszélyeztetésének speciális, nevesített esete. Jogi tárgyként a kiskorú nemi érését biztosító egészséges testi, szellemi, erkölcsi fejlődése fogalmazható meg. Kiskorú személynek tekinthető a büntetőjog szempontjából a 18. életévet be nem töltött személy. A bűncselekmény tárgyi elemei közül az elkövetési magatartás a pornográf jellegű képfelvétel készítése, forgalomba hozatala, illetőleg ezzel való kereskedés. Készítés fogalmán az ilyen tárgyú video-, film- valamint fényképfelvételek bármilyen technikával történő előállítását, megjelenítését értjük. Mivel a grafikai ábrázolásra nem utal a törvényhely, így a kiskorúról készült pornográf grafika kívül reked a tényállás keretein. A forgalomba hozatal nemcsak e felvételek átadása, ajándékozása jelenti, hanem tág értelemben minden olyan magatartást, amellyel mások számára hozzáférhetővé teszi a felvételt, így *a nagy nyilvánosságot lehetővé tevő hálózaton való elérést is.* Azt gondolom, hogy ezt a körülményt a bíróságnak a súlyosító körülményként kell értékelnie. A kereskedés a forgalomba hozatalnál szélesebb körű tevékenység, amely magában foglalja az ilyen felvételek forgalmazásában való közreműködést (pl. szervezést, közvetítői tevékenységet, e felvételek továbbítását stb.) A (3) bekezdésben egy delictum sui generis fizikai bűnsegédi alakzatot határoz meg. Az anyagi eszközök szolgáltatása felöleli e tevékenységhez való pénz-, és technikai eszközök (pl. számítógép vagy képolvasó) biztosítását.

D. Visszaélés kábítószerrel

"282. § (9) Aki ..... b./ nagy nyilvánosság előtt kábítószer - fogyasztásra hív fel, ha súlyosabb bűncselekmény nem valósul meg, vétséget követ el, és két évig terjedő szabadságvesztéssel büntetendő."

A kábítószer fogyasztására irányuló és meghatározatlan számú személy által elérhető felhívás azt a veszélyt rejti magába, hogy felkelti a kábítószer fogyasztás

iránti érdeklődést. A felhívás tartalmában lehet a kábítószerek fogyasztásának, fajtáinak, elérhetőségének, árainak stb. népszerűsítése.

E. Háborús uszítás

"153. § (1) Aki háborúra uszít vagy egyébként háborús hírverést folytat, bűntettet követ el, és két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés öt évtől tizenöt évig terjedő szabadságvesztés, ha a bűncselekményt nagy nyilvánosság előtt követik el.

(3) Aki háborús uszításra irányuló előkészületet követ el, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."

A háború propagálását a Polgári és Politikai Jogok Nemzetközi Egyezségokmány - amely 1976. óta része belső jognak - 20. cikkének 1. pontja kimondja: "Minden háborús propagandát törvényben kell megtiltani." A háborús hírverés az uszításnál szélesebb fogalom. Minden olyan közlés a számítógépes hálózatokban, amely háborús propagandát szolgál e bűncselekmény megállapítására alkalmas lehet. Míg az uszítás egy egyszeri magatartással is megvalósítható, addig a hírverés folytatása több alkalom meglétét tételezi fel.

7. A BÜNTETŐ ELJÁRÁSJOG-TUDOMÁNYT ÉRŐ KIHÍVÁS

Az anyagi büntetőjog szabályai, amelyek meghatározzák a bűncselekménynek minősülő cselekményeket, az elkövetőkkel szemben alkalmazható szankciókat és a szankciók alkalmazásának feltételeit az alaki büntetőjogban, más terminológiával a büntető eljárásjogban jut érvényre, annak szabályrendszerében realizálódik. **Tremmel Flórián** szerint ez a büntető eljárásjognak egyik *külső funkciója.*[253] Ebben a - vázlatos - összefüggésben az anyagi büntetőjogi szabályok, mint a büntetőigény feltételei a *statikus* összetevője, míg ezek érvényesülésének módját megállapító büntető eljárásjog a büntetőjog *dinamikus* összetevője az alaki büntetőjog. **Angyal Pál** örökbecsű szavait idecitálva "az alaki büntetőjog valósággal lelket lehel az anyagi büntetőjogba."[254] Ez a szoros konnexió többek között azt is jelenti, hogy az anyagi büntetőjogban beálló módosulás, amelyet akár politikai - gazdasági fordulat, akár műszaki - technikai haladás indukál, vagy akár az ezeken túlnövő kriminálpolitikai megfontolások érvényre juttatása szükségképpen érinti eljárásjogi szabályokat, vagy azok megreformálása válik szükségessé, vagy legalábbis a felelősségrevonás eddigi szabályozott menete módosul. Ahogy az anyagi büntetőjogi szabályozásban az anyagi büntetőjog-tudomány eredményei öltenek testet, kelnek életre, úgy a saját normarendszerrel bíró eljárásjog is a büntető eljárásjog - tudományból merít. A számítógépes környezetben elkövetett bűncselekmények, nemcsak az "anya-tudomány" számára jelentettek új kihívást, hanem az eljárásjog tudományt, és a kriminalisztikát sem hagyhatja figyelmen kívül. A számítógépes adatok "testetlensége", "láthatatlansága", mint ezen bűncselekményi kör specifikumai az anyagi büntetőjog-tudományt új tényállások megalkotására ösztönözték. Ugyanezen okból eredően, a számítógépes adatok, mint bizonyítékok beszerzéséhez, vizsgálatához nem minden esetben nyújtanak kielégítő megoldást a tradicionális eljárásjogi szabályok. Ne feledjük, hogy ezen "testetlen",

---

[253] Dr. Tremmel Flórián: Büntető eljárásjog. Általános rész. Pécs, 1996. 8.l.
[254] Dr. Angyal Pál: A magyar büntetőeljárásjog tankönyve I. kötet. Budapest, 1915. 3.l.

"láthatatlan" elektronikus adatok megjelenítéséhez technikai eszközökre van szükség, tartalmukban a privátszféra érzékeny információit rejthetik.

Ma már a hagyományos köznyugalom-, vagyon elleni, gazdasági vagy más bűncselekmények nyomozásakor is szükség lehet számítógép memóriájában tárolt adatok, programok megismerésére, egyéb adathordozók lefoglalására, terheltek vagy tanúk együttműködésére. A nyomozó hatóságok személyi és technikai felkészültségének elérése szintén kiemelten fontosságú. A sikeres büntető eljárás véghezviteléhez a nyomozó hatóság szellemi és technikai fölényben kellene kerülnie. A német **Ulrich Sieber** az eljárásjog-tudományt érő kihívásokat a következőképpen osztályozza:- a büntető eljárás során megjelenő passzív tűrési kötelezettségek(számítógép átvizsgálása, adatok lefoglalása, a számítógépek közötti kommunikáció rögzítése stb.), valamint- aktív közreműködési kötelezettségek (terhelt, tanú) újragondolása, végül- a nyomozás során feltárt adatok védelme.[255]

E nem kevés dilemma feloldását segítendő az *Európa Tanács* 1995-ben kibocsátja *13. sz. Ajánlását* az információs technológia által felvetett büntető eljárásjogi problémákkal összefüggésben. Ez a dokumentum számos a büntető eljárásjogban felvetődő, többnyire praktikus problémát vesz górcső alá, így a házkutatás és a lefoglalás az eljárásban részvevők együttműködési kötelezettsége, a bizonyítékok értékelése stb. Az ET. (95) 13. sz. Ajánlása az alábbiak megfontolását javasolja a tagállamok számára:"*A műszaki ellenőrzésről*

5. Tekintettel az informatika és a telekommunikáció közötti szoros kapcsolatra, a büntetőjogi eljárásban alkalmazott műszaki ellenőrzésre vonatkozó rendelkezéseket, - mint például *telekommunikáció lehallgatása*, - felülvizsgálatra és módosításra szorulnak, ahhoz hogy alkalmazhatók legyenek.

6. A törvényben engedélyezni kell a nyomozó hatóságnak, hogy igénybe vegyen minden olyan műszaki eszközt, amely a nyomozáshoz szükséges *adatok megszerzését* lehetővé teszi.

---

[255] Dr. Ulrich Sieber: Computerkriminalität und Informationsstrafrecht. Computer und Recht 11. 1995. s. 109- 110.

7. A nyomozás során gyűjtött adatokat, különösen, ha az adatgyűjtés valamilyen telekommunikációs eszköz lehallgatásával történt, *jogi védelem* alá kell helyezni és megfelelő módon őrzött számítógépes rendszeren kell tárolni.

8. A büntetőjogi törvényeket úgy kell átdolgozni, hogy lehetővé tegyék a telekommunikációs eszközök lehallgatását és az adatforgalom összegyűjtését a telekommunikációs eszközök és a számítógépes rendszerek titkossága, épsége és hozzáférhetősége ellen elkövetett súlyos vétségek esetén történő nyomozásban. *A nyomozó hatóságokkal való együttműködési kötelezettségről*

9. A legtöbb jogrend megengedi a nyomozó hatóságnak, hogy jogi kiváltságok vagy védelem fejében utasítson embereket arra, hogy átadják neki a birtokukban levő tárgyakat, amennyiben azokat bizonyítékként kívánja felhasználni. Ezzel párhuzamosan gondoskodni kell arról, hogy a nyomozó hatóságnak felhatalmazása legyen arra, hogy *elrendelje* bárkinek a birtokában levő számítógépes rendszeren tárolt *adatok átadását* a nyomozáshoz szükséges formában.

10. Jogi kiváltságok vagy védelem biztosítása ellenében a nyomozó hatóságnak felhatalmazása kell legyen arra, hogy *utasítsa* azokat, akik számítógépes rendszerükön adatokat tárolnak, hogy megadják a hatóságnak a *szükséges információkat* ahhoz, hogy hozzáférjen a rendszerhez és a tárolt adatokhoz. A büntetőjogi törvényeknek biztosítani kell, hogy hasonló utasítást lehessen adni azoknak, akik megfelelő ismeretekkel rendelkeznek a számítógépes rendszerek működésével kapcsolatban vagy biztosítani tudják a tárolt adatok védelmét.

11. Külön *kötelezettséget* kell róni a telekommunikációs szolgáltatást nyújtó köz- és magántulajdonban levő hálózatok operátoraira, hogy minden lehetséges technikai eszközzel *segítsék* a nyomozó hatóságokat a telekommunikáció *lehallgatásban.*

12. Külön *kötelezettséget* kell róni azokra a *szolgáltatókra*, akik telekommunikációs szolgáltatást nyújtanak a nyilvánosság számára a köz- és magántulajdonban levő

hálózaton keresztül, hogy illetékes nyomozó hatóság felszólítására megadjanak a hatóságnak minden információt a felhasználó *azonosítására.....*" [256]

7. 1. A büntető eljárásjogi kényszerintézkedésekről általában

A büntető eljárás sikerét a bűncselekmény teljeskörü felderítése, bizonyítása jelenti. Ez alapozhatja meg az aggálymentes bírói döntést az elkövető eljárásjogi bűnösségében. E cél érdekében szükséges olyan kényszerintézkedések biztosítására, amelyek a büntető eljárás különböző, de egymás épülő szakaszaiban a hatóságok rendelkezésére állnak. A kényszerintézkedések lehetnek személyi-, illetőleg tárgyi kényszerintézkedések. Azaz egyes személyek, általában a terhelt jelenlétét, de a bizonyítás szempontjából nélkülözhetetlen személyek jelenlétet biztosító vagy a bizonyítás eredményességéhez szükséges tárgyak, helyszínek megismerését szolgáló intézkedések megtételére nyújt lehetőséget a büntető eljárási törvény. Minden kényszerintézkedés az emberi és állampolgári jogokat érinti, azokat korlátozza. **Hazánkban** az 1949. évi XX. sz. törvény, az Alkotmány az alapvető emberi és állampolgári jogokat deklarálja: *"A Magyar Köztársaságban mindenkit megillet a jó hírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog."* Ezen jogokat számos további törvény (pl. a Polgári Törvénykönyv, az Adatvédelmi törvény) konkretizálja, részletezi és meghatározza az azok megsértőikkel szemben alkalmazható szankciókat. E jogok korlátozásának feltételeiről - a témát tekintve - az alábbi törvények rendelkezései nyújtják a keretet:

"A büntetőeljárásban a személyi szabadságot és más állampolgári jogokat tiszteletben kell tartani, s azok csak e törvényben meghatározott esetekben és módon korlátozhatók." (Be. 4. § (1) bekezdés.)

"A Rendőrség a feladatának ellátása során a testi épséghez, a személyes szabadsághoz, a magánlakás, a magántitok és a levéltitok sérthetetlenségéhez, a

---

[256] Recommendation No. R (95). 13 of the Committee of Ministers to Member States - Concerning Problems of Criminal Procedure Law Connected with Information Technology. www.usdoj.gov/criminal/cybercrime/crycoe.htm vagy www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html

személyes adatokhoz valamint a tulajdonjoghoz fűződő jogokat a törvényben foglaltak szerint korlátozhatja." (Rtv. 17. § (1) bekezdés.)

E citátumokból látható az, hogy az emberi és állampolgári jogok korlátozása *csak* törvényben meghatározott esetekben lehetséges. A Rendőrségi törvény részletezi azt, hogy milyen jogok korlátozására számíthat(nak) a büntető eljárás alá vont személyek. A Büntető eljárási törvény ellenben nem részletező, amelynek oka minden bizonnyal az, hogy az alapelveket deklaráló rendelkezések közé nem illik egy ehhez hasonló felsorolás.

Az emberi és állampolgári jogok a fenti törvényhelyeken meghatározott kényszerintézkedések alkalmazása során szükségképpen csorbulhatnak. Nem mindegyik kényszerintézkedés korlátozza az állampolgári jogokat ugyanolyan mértékben, hanem azokat eltérően is érintheti. A kényszerintézkedések lényegét az alábbiakban definiálható: "a büntető ügyekben eljáró hatóságok által a büntetőeljárás sikere érdekében, eljárási célokra, a büntető-eljárási törvényben meghatározott esetekben és módon alkalmazható, kényszer tartalmú intézkedések, amelyek szükségszerűen az alapvető állampolgári jogoknak, az ún. emberi jogoknak különböző mértékben való korlátozásával járnak." [257] A számítógépes környezetben elkövethető bűncselekmények esetében azon kényszerintézkedésekkel szükséges foglalkoznom, amelyek alkalmazásuk során bizonyos sajátosságot mutatnak. A kényszerintézkedések céljukat tekintve tárgyi bizonyítékok megszerzésére irányulnak, ezek a házkutatás, illetőleg a lefoglalás.

7. 2. A házkutatásról

A házbéke jogát már a római jog is védelmezte, realiniuriaként a becsületsértés egyik eseteként (domum vi introire) ismert és elismert esete, majd a francia Code Penaltól általánosan védett a kontinensen. **Hazánkban** a házbéke jogát az Alkotmány deklarálja. Megsértése esetére más törvények határoznak meg szűk körű szankciókat (pl. a Ptk-ban a birtokvédelem lehetősége, a Btk-ban magánlaksértés szankcionálása). A házbéke jogának csorbulását jelenti a büntető

---

[257] Dr. Tremmel Flórián: Büntető eljárásjog id. mű ... 260.l.

eljárási törvényben szabályozott házkutatás intézménye.

E büntető eljárásjogi intézmény célja a bűncselekmények sikeres felderítésének céljából a gyanúsított, esetleg más személy (egyszóval az érintettek) kézrekerítése, avagy bűncselekmények nyomainak felderítése, valamint tárgyi bizonyítékok felkutatása. E két utóbbi fordulat realizálása a számítógépes környezetben elkövetett bűncselekmények során mutat némi sajátosságot. Tekintsük át először az eljárásjogi problémákkal foglalkozó Európa Tanács idevonatkozó megállapításait:

"*A házkutatásról és a lefoglalásról*

1. Pontosan ismertetni kell a számítógépes rendszerek átkutatása, a tárolt adatok lefoglalása valamint a lehallgatás közötti különbséget és azt a gyakorlatban alkalmazni kell.
2. A büntetőjogi törvényekben a házkutatás és a lefoglalás hagyományos gyakorlatának megfelelő módon engedélyezni kell, hogy a hatóságok meghatározott körülmények között átvizsgálhassanak számítógépes rendszereket és lefoglalják az itt tárolt adatokat. A rendszerért felelős személyt tájékoztatni kell arról, hogy a rendszert átkutatták és milyen adatokat foglaltak le. A számítógépes rendszerek átkutatása és az adatok lefoglalása esetén is ugyanazt a jogorvoslatot kell alkalmazni, mint házkutatással és lefoglalással szembeni általános jogorvoslatot.
3. A házkutatás során a nyomozó hatóságot olyan hatáskörrel kell felruházni, hogy megfelelő védelem biztosítása ellenében kiterjessze a házkutatást más számítógépes rendszerekre is, amelyek a hálózatra csatlakoznak és hogy lefoglalhassa az ott tárolt adatokat is, amennyiben azonnal intézkedésre van szükség.
4. Ahol az automatikusan feldolgozott adatoknak megfeleltethető egy hagyományos dokumentum, ott a dokumentumok átvizsgálására és a lefoglalására vonatkozó büntető törvényeket kell alkalmazni."[258]

A házkutatás foganatosításával összefüggő szabályok jellegzetessége az, hogy egyfelől vannak *kizárólag* a házkutatásra vonatkozó szabályok, másfelől a motozásnál és lefoglalásnál *is* irányadó normák. Ez utóbbiak közé tartozik az

[258] CE Recommendations (95) 13. (v.ö. 204.sz.)

érintett kíméletének követelménye, a kényszerintézkedés jegyzőkönyvezésének kötelezettsége, valamint a rendbírság alkalmazásának lehetősége ezen kényszerintézkedést akadályozókkal szemben. (Lásd részletesen Be. 105. §-ban.) A magyar büntető eljárásjogban házkutatás helyei lehetnek: ház, lakás, egyéb helyiség, ezekhez tartozó bekerített hely, továbbá jármű (Be. 103. § (1) bekezdés).

Az ET. ezen ajánlásával - de lege ferenda - szükségesnek mutatkozik az 1973. évi I. törvény 103. § (1) bekezdésének olyan módosítása, amely a házkutatás helyei (tárgyai) között szerepeltetné az "elektronikus adatfeldolgozó rendszert". Ez a nevesítés azért fontos, mivel ez, mint rendszer *nem lokalizálható* egy helyiségben. A nyomozó hatóság akár saját számítógépükről belépve kutathatják át pl. az Interneten elérhető bűncselekmény alapos gyanúját megalapozó pornográf, gyűlöletkeltésre stb. alkalmas adatállományokat, továbbá ezen rendszeren átmenő információk lehallgatását. E kiegészítéssel a büntető eljárási törvényünk az ET. ajánlásának fentebb I. 3. pontjában írt követelményével *konform* lenne. Az Ajánlás I.2. pontjában említett tájékoztatási kötelezettség már szerepel törvényünkben, mégpedig bármilyen bűncselekménnyel kapcsolatban: "A házkutatást rendszerint az érdekelt jelenlétében kell elvégezni; megkezdése előtt közölni kell vele a házkutatást elrendelő határozatot és fel kell őt szólítani, hogy a keresett tárgyat önként adja elő." (Be. 103. § (2) bekezdés). Itt kell megjegyeznem, - és ez már átvezet a *kriminalisztikai* kérdéskörhöz, - hogy a "keresett tárgy önkéntes kiszolgáltatása" sem jelentheti azt, hogy a gyanúsított a számítógép billentyűzetét kívánja használni. Bár valamennyi bűncselekmény felderítése érdekében alkalmazott házkutatást alaposan meg kell szervezni, ám a számítógépes környezetben elkövetett deliktumok gyanúja során további teendő; szakértő vagy szaktanácsadó részvételének biztosítása, amely nem minden deliktum esetében szükséges, ám e körben nélkülözhetetlen. A hagyományos nyomrögzítő eszközök mellett adatrögzítő eszközök alkalmazása elengedhetetlen. Majdan ezzel rögzíthetők a számítógép memóriájában tárolt adatok. Ismerni kell azt, hogy a bűncselekmény elkövetésének eszköze a számítógép volt-e vagy a cselekmény extra-, intra- illetve Internetes

hozzáférés révén valósult-e meg. Ugyanígy előrevivő az előzetes adatgyűjtés során kitudakolni az érintett(ek) által használt szoftvereket (operációs rendszereket, szövegszerkesztő, táblázatkezelő vagy más programokat). A házkutatás végrehajtásának első fázisát, a házba, a lakásba, más helyiségbe vagy ezekhez tartozó bekerített helyre történő bejutást követően az érintett(ek) - esetleges - fizikai ellenállásának megtörésén túl, ahogy fentebb említettem, annak megakadályozása elérendő, hogy az érintett(ek) a számítógéphez vagy az elektromos hálózati kapcsolóhoz férjenek. Elegendő egyetlen gomb megnyomása, egyetlen az érintett(ek)től származó hamis jelszó (password) begépelése, amelyek egy vírusprogramot aktivizálhatnak és törölheti azon adatállományokat, ami a bizonyíték forrása lehet. A házkutatás révén a nyomozó hatóság tárgyi bizonyítékokra is szert tehet, de a házkutatás alkalmas arra, hogy az érintett személy életkörülményeibe is bepillantást nyerhessen a nyomozó hatóság.

Ehhez kapcsolódóan fel kell tenni azt a kérdést, hogy az elektronikus adatfeldolgozó rendszerbe történő belépés házkutatásnak vagy szemlének minősüle? A *házkutatás* célja a tárgyi bizonyítékok, továbbá a bűncselekménnyel összefüggésbe hozható nyomok felkutatása. A *szemlének,* mint szintén büntető eljárási cselekménynek nem célja a tárgyi bizonyítékok fellelése, hanem "személy, tárgy vagy helyszín közvetlen megtekintése" (Be. 84. §) a cél, annak érdekében, hogy ezen nyomok (vagy anyagmaradványok) egy további vizsgálatot követően alkalmasak a bűncselekményben betöltött szerepének a tisztázására. Leegyszerűsítve a házkutatás a tárgyi bizonyítékok felkutatásának célja, a szemle ennek eszköze. E két kényszerintézkedés nem mindig határolható el élesen egymástól; pl. a hatóság által ismert helyen feltalálható tárgynak a bűncselekményben való relevanciája kérdéses.[259]

7. 3. A lefoglalásról

A lefoglalás olyan tárgyi kényszerítő cselekmény, amelynek során a lefoglalt, fizikai léttel bíró, tehát tárgyiasult testi dolgot annak tulajdonosától vagy

---

[259] Matus Márk: Illetékesség c. tanulmány kézirata 1-2.l.

birtokosától elvonja. E dolog lehet a bűncselekmény eszköze, produktuma vagy objektuma. A lefoglalás célja általában túlnő a büntető eljárás eredményességének biztosításán, mivel e lefoglalt dolgok válnak az elkobzás, mint büntető anyagi jogi szankció (intézkedés) tárgyaivá. Ez utóbbira figyelemmel, a lefoglalt dolgok biztosítása a büntető anyagi jogban is relevanciával bír(hat). Az adatok gyűjtése során nemcsak az adathordozók birtokbavétele, hanem a számítógépben találhatók adatok megszerzése, sőt a hálózatok átkutatása is szükségessé válhat.

Először azt kell megválaszolnom, hogy mi a lefoglalás tárgya a számítógépes bűncselekmények esetében? Majd arra kell választ adnom, hogy önmagában az inkriminált adatállomány kimásolása a nyomozóhatóság által vitt adathordozóra lefoglalás-e vagy sem? A kérdések megválaszolásához vázlatosan tekintsük át lefoglalás technikai megvalósulását: a házba, lakásba, egyéb helységbe történő bejutást követően jutnak szerephez a szakértők vagy szaktanácsadók. Számítógépes csalás (Btk. 300/C. §) esetében a számítógép memóriájában tárolt adatállomány elérése az operációs-rendszer-, a meghajtó-, a könyvtár-, majd az inkriminált file-ok azonosításán vezet az út. ("Természetesen" fel kell készülni, a különböző szintű hozzáférést védő jelszók nem kevés gondot okozó megfejtésére, és néhány sikertelen kísérlet esetében a számítógép leállására.) A bűncselekmény felderítésének sikere érdekében ajánlatos már a könyvtárállományt is rögzíteni adathordozón, kinyomtatni nyomtatón, esetleg lefotózni. Az inkriminált adatállomány elérését követően, mivel az "láthatatlan" a külvilág számára, "testetlensége" folytán nem vehető birtokba, úgy megjeleníthető képernyőn való kiíratás vagy nyomtatás által, illetőleg a nyomozóhatóság hatóság által előkészített adathordozóra másolható. Az első kérdésre a válasz a büntető eljárási törvény definíciójában rejlik. Lefoglalás tárgya csak tárgyi bizonyítási eszköz (Be. 101. § (1) bekezdés). Ilyen tárgyi bizonyítási eszköz csak adathordozó lehet. Tehát nem számítógépes adat foglalható le, hanem az az adathordozó, amelyen az adat rögzítve van. A német Wolfgang **Bär** szerint "a nyomozás szempontjából meghatározó információk ..... csak a tárgyiasult adathordozóval együtt, mint a

legkisebb *önállósítható egységgel* együtt foglalhatók le." [260]Lefoglalható továbbá a számítógépe merevlemeze. Remélhetően egyre ritkább a lefoglalás azon módja, amikor magát a számítógépet foglalják le. Az egyes adatállományok átmásolása kisebb intenzitású beavatkozást jelent, mint a merevlemez vagy az egész gép elvitele. Visszatérve **Wolfgang Bär**hez, megállapítja továbbá, hogy "a számítógépes berendezések, a számítógéppel nyomtatott iratok és az adathordozók is, mint testi tárgyak a lefoglalás releváns objektumai képezik."[261]

A második kérdésre a válasz a lefoglalás funkciójából ered. A lefoglalás a bűncselekményben szerepet játszó dolog vagy dolgok birtokosától történő ideiglenesen elvonása. Azzal, hogy a nyomozó hatóság tagjai a számítógépből kimásolják az inkriminált adatállományokat egy adathordozóra, azok továbbra is az érintett "birtokában" maradnak. Ezen adatállományok akkor kerülnek ki az érintett birtokából, ha azokat a rögzítés követően azonnal törlik a számítógép memóriájából. Tehát bár a lefoglalás tárgya csak adathordozó lehet és nem a számítógép memoárjában tárolt adat, de lefoglalásról akkor beszélhetünk, ha az érintettet megfosztják a számítógép memóriájában tárolt adatoktól. A szerzői és szomszédos jogok megsértése (Btk. 329/A. §) bűncselekményének nyomozásakor nem szükséges a számítógépes programot kimásolni egy adathordozóra, véleményem szerint elegendő a program behívását követően annak azonosítását jelző oldal rögzítése. Különösen akkor, ha maga a program írja ki, hogy "unregistered program", „unregistered version" stb. Ezt követően a programot - általában - törölni szükséges az érintett számítógépéről. Ennek generálissá tétele azonban rendkívül nehézséget is okozhat az érintett számára. Pl. egy illegális szoftveren van egy vállalkozás, vállalat könyvviteli, értékesítési, leltári folyamata, annak adatai stb. Ezáltal előfordulhat az az eset, hogy a szoftver törlése a bűncselekmény tárgyi súlyához képest *aránytalan sérelmet* okoz. Ennek elkerülésére mindenképp törekedni kell. Ennek érvényre juttatására hív fel a Rendőrségi tv. 15. § (1)

---

[260] Wolfgang Bär: Beschlagnahme von Computerdaten (II). Computer und Recht 12. 1996. s. 752.

[261] Wolfgang Bär: id. mű .... s. 752.

bekezdése, miszerint "a rendőri intézkedés nem okozhat olyan hátrányt, amely nyilvánvalóan nem áll arányban az intézkedés törvényes céljával," illetőleg erre utal a Be. 105. § (1) bekezdésének utolsó fordulata is, miszerint a tárgyi kényszerintézkedések alkalmazása során "kerülni kell a szükségtelen károkozást". Elképzelhető a nyomozás időtartamára a program biztosítása akként, hogy azt ne lehessen törölni.

A számítógép memóriájában vagy az adathordozókon tárolt adatok a bíróság által történő közvetlen észlelése nem lehetséges, csak más technikai eszköz közbeiktatásával. "Ha a nyomoknak a bíróság részéről történő közvetlen szemlélésére nem kerülhet sor",[262] *származékos bizonyítékokról* beszélünk. Ezen adatok hitelességének biztosítása rendkívül fontos mind a nyomozó hatóság, mind az érintett számára. Ez lehet az alapja az igazság elérésének, mint a büntető eljárásjog további külső funkciójának érvényesülésének.[263] A hitelesség - de lege ferenda - akként lenne biztosítható, ha a számítógépben tárolt adatokat két adathordozóra is rögzítik, majd azokat lezárt borítékokba helyezik, feltüntetik rajta az eljárási cselekményre vonatkozó adatokat. A leragasztott, lepecsételt, hatósági tanúk által hitelesített borítékokból az egyik a nyomozás felügyeletet ellátó ügyészség, a másik a nyomozó hatóság számára szolgál bizonyítékul. Ezáltal a bizonyítékok koholásának lehetőségét kizárhatnánk. E praxisból származó megoldás jogi köntösbe öltése szükséges.

A számítógépes adatok megjeleníthetők nyomtatással egy papírlapon, kiírathatók képernyőn, ezáltal lefényképezhető. Az inkriminált állapotot tükröző adatsor- vagy halmaz, ábra, grafika, szöveg stb. ezáltal jeleníthető meg a külvilágban, válik szemmel érzékelhetővé, láthatóvá. Az elektronikus impulzus megjelenítése a látens nyomokkal mutat hasonlóságot. Igaz a látens nyomok létjogosultságáról megoszlik a kriminalisztikai szakma véleménye.[264]

---

[262] . Dr. Katona Géza: A nyomok azonosítási vizsgálata a büntetőeljárásban, Budapest, 1965. 15.l.

[263] Dr. Tremmel Flórián: Büntető eljárásjog ... id. mű 8.l.

[264] pro: Dr. Tremmel Flórián - Dr. Fenyvesi Csaba: Kriminalisztikai tankönyv és Atlasz. Budapest 1998. 40.l. contra: Dr. Katona Géza: id. mű 43.l.

A kinyomtatott papír, a képernyőről készített fénykép megfelel a **magyar büntető-eljárási** törvényben tágan értelmezett tárgyi bizonyíték fogalmának (Be. 82. § (2) bekezdés). A számítógépes adatok egy hangszintetizátor segítségével emberi beszéddé is formálható és így mágnesszalagra rögzíthető. Bár ez a megoldás még nem tekinthető általánosnak. A mágnesszalagon levő szöveg bizonyítóereje kétséges, ezért bíróságaink azt nem is fogadják el bizonyítékként, hiszen könnyedén "összevágható", manipulálható. Az adatrögzítés által nem jönnek létre új bizonyítékok, hanem a ma már megvolt bizonyítékok válnak általánosan megismerhetővé, tartósan hozzáférhetővé az eljárás céljára. Mivel az adathordozók (számítógépes merevlemez, hajlékony lemez, mágnesszalag, lyukkártya- vagy szalag) - testi, és birtokba vehető dolgok - így megfelelnek a tárgyi bizonyíték fogalmának, ezáltal azok a hatályos szabályok szerint lefoglalhatók.

Rendkívül kényes problémát vet fel a lefoglalható adatok körének meghatározása. Figyelemmel arra, hogy egy - egy adathordozón több százezer bit információ tárolható, így a nyomozás szempontjából érdektelen adatokhoz is hozzáférhetnek a nyomozó hatóságok. Az adatok kezelésére több törvény szigorú szabályai vonatkoznak. A Be. 105. § (1) bekezdése a lefoglalás, a házkutatás és a motozás közös szabályai között kiemeli a nyomozás során előkerült magántitkok megőrzésének kötelezettségét. Ebbe a körbe tartoznak nemcsak a természetes személyek érzékeny adatai, hanem jogi személyek és más szervezetek titoknak minősülő adatai is. A **rendőrségi törvény** (1994. évi XXXIV. törvény - Rtv.) a bűnüldözési és az államigazgatási feladatokhoz kapcsolódó adatok kezelésének feltételeit rögzíti. A bűnüldözés céljából gyűjtött és tárolt adatokat csak rendőrségi valamint bűnüldözési célra használható, kivéve ha e törvény másként nem rendelkezik (Rtv. (77. § (1) bekezdés).

A rendőrség felhasználhat más szervek által kezelt személyes adatokat is bűnüldözés céljára. Ezeket azonban e fenti céltól eltérően nem használhat és azokat nem továbbíthatja (Rtv. 77. § (2) bekezdés). E törvény értelmében a rendőrség kötelessége, hogy az adatalany a rendőrség által kezelt adatokhoz hozzáférhessen, azokat helyesbíthesse, törölhesse. Ugyanakkor a tárolt adatokat törölni kell, ha azok

kezelésének oka megszűnt vagy a bíróság az adatok törlését elrendelte (78. § (2) bekezdés a. és b. pontjai). A számítógépes adatok lefoglalása kapcsán a magyar büntető-eljárási törvény módosítása válik szükségessé. E szupplementummal garanciák beemelése is nélkülözhetetlen. De lege ferenda tehát egyrészt csak, és kizárólag az ügy érdemi elbírálásához *elengedhetetlen adatállományok* vizuálissá tételének követelményét kellene expressis verbis kimondania büntető-eljárási törvénynek. Bár a Be. tárgyi kényszerintézkedések közös szabályait rögzítő 105. § (1) bekezdésében meghatározza azt, hogy "biztosítani kell, hogy az intézkedés folytán ne kerüljenek nyilvánosságra a magánéletnek az üggyel össze nem függő körülményei", ám gazdálkodó szervezetek, intézmények érdekeire (az üzleti, szolgálati, banktitkokon túlmenően) is figyelmet kellene fordítani. Másrészt fontos lenne a nyomozás céljára lefoglalt adathordozók lefuttatatásának, kinyomtatásának *ügyészi felügyelethez* kötése.

7. 4. A lehallgatás

A számítógép-rendszerek lehallgatásának nemcsak az átvitt adatok megszerzése lehet a célja, hanem a tranzitadatok is (pl. e-mail üzenetek), amely felveti a távközlési hálózatok, különösen az országon áthaladó hálózatok lehallgatásának lehetőségét. Mivel a számítógépes adatok technikailag többféleképpen tárolhatók (a számítógépekben, adathordozókon, hálózatokban stb.) így nem egyértelmű, hogy a számítógépeket- vagy hálózatokat az adatok, mint bizonyítékok megszerzése céljából lehallgatják-e vagy átkutatják. Csupán utalok arra, hogy egyes országokban a lehallgatás, mely a telefonvonalak megfigyelését jelenti, szigorúbb szabályok között eszközölhető, mint más a bizonyíték megszerzésére irányuló nyomozati cselekmény. Ennek előrebocsátását követően az európai joggyakorlat részleges áttekintése kapcsán alábbi kérdések vethetők fel?

1. Van-e jogi következménye az adatátviteli formák közötti különbségnek?
2. Mi a különbség a számítógép- és rendszer lehallgatása és átvizsgálása között?
3. Van-e különbség köz(szolgálati) és magánhálózatok lehallgatásának?

Ad 1. A számítógépes és egyéb kommunikációs formák közötti különbségtételt nem mindig követte, követi a jogi és ezen belül a büntetőjogi szabályozás. Az egymástól nagy távolságra levő számítógépek kommunikációjának megteremtésével a szóbeli érintkezést szolgáló telefonhálózatok mellett egy új kommunikációs forma is létrejött. A számítógépes és egyéb kommunikációs hálózatok közötti meglevő technikai különbség eltérően jelenik meg a nemzetközi joggyakorlatban.

a. Az országok egyes csoportjaiban különbséget tesznek a számítógépes- és a telefonhálózatok lehallgatásának feltételei között. A **német** a büntető eljárási törvény 100a. - 100b. §-ai[265] továbbá az 1986-os egyesült államokbeli Elektronikus kommunikáció titkosságáról (Electronic Communications Privacy Act) szóló törvény[266] meghatározzák a számítógépes kommunikáció lehallgatásának feltételeit. Az 1985-ös Brit Lehallgatási Törvény (British Interception of Communications Act) is több egymás mellett létező kommunikációs formát ismer el (1. §).[267]

b. A kommunikációs technikák sokrétűségétől függetlenül a **holland** büntető eljárási kódex 125g. § arról rendelkezik, hogy a vizsgálóbíró elrendelheti bármely kommunikációs hálózat lehallgatását. E szakasz alapján idetartozik nemcsak a telefon, hanem a telefax, telex és a számítógépes adatátviteli vonalak is.

"125g. § Előzetes törvényszéki nyomozás során a vizsgálóbíró felhatalmazása alapján a nyilvánosság számára nem hozzáférhető és a telekommunikációs infrastruktúrán átmenő adatok lehallgathatók vagy rögzíthetők."

A majdani hazai törvényhozás számára is követendő az a szabály, amely szerint *"a vizsgálóbíró jelenlétében haladéktalanul meg kell semmisíteni azon hivatalos jelentéseket, tárgyakat, amelyek a 125f. és a 125g. § alapján lehallgatás*

---

[265] Revue ... p. 353.

[266] Revue ... p.666.

[267] www.man.ac.uk/MVC/SIMA/legal/intercep.html

vagy rögzítés útján keletkeztek és a nyomozás szempontjából érdektelenek. A megsemmisítésről késedelem nélkül jelentés készítendő."[268]

c. Viszont vannak országok, ahol a "hagyományos" lehallgatás előírásait alkalmazzák (terjesztik ki) a számítógépes kommunikáció figyelésére. Így a **német** büntető perrendtartás 100.a és 100.b §-ok szabályai szerint a bíró, ha az engedélyezés a nyomozás sikerét veszélyeztetné, úgy az ügyész 72 óra időtartamra engedélyezheti a telekommunikációs vonalak lehallgatását. Ez magában foglalja a tárolt vagy az átmenő (tranzit) adatok rögzítését is.[269]

Ad 2. A bizonyítékul szolgáló adatok megszerzése számítógépek lehallgatása és átkutatása (mint házkutatás) révén realizálódhat. Mi a különbség a kétféle kényszerintézkedés között? A számítógépes hálózatokról már tudjuk, hogy azok lehetnek lokális hálózatok vagy nagytávolságú hálózatok. A számítógépes kommunikáció bonyolódhat telefonvonalakon, rádiófrekvencián, adatátviteli vezetéken vagy műholdon keresztül. Lehallgatásról akkor beszélünk, ha a számítógépes adatot (szöveget, képet, hang-file-t stb.) a számítógépeket összekötő hálózatból szerzik meg rádiójelek azonosításával, telefonvonalak hullámrezgéseinek rögzítésével, adatátviteli vonalak megcsapolásával vagy más módon. A számítógépek- vagy hálózatok átkutatása - ahogy azt fentebb már láttuk a házkutatásról szóló fejtegetésben - a számítógép merevlemezének, továbbá a hajlékony- és kompaktlemezek, mágnesszalagok, lyukkártyák- és szalagok tartalmának kitudakolását jelenti.

Ad 3. Információt nemcsak állami-, közcélú szolgáltató-, hanem magánhálózatok is továbbítanak. A **holland** büntető eljárási törvény 125. f. - h.

---

[268] www.minjust.nl:8080/C__ACTUAL/PERSBER/compcrim.htm - saját fordításban.

[269] Revue ... p. 353.

szakaszai alapján a nyomozóbíró elrendelheti az állami hálózat lehallgatását. A magánhálózatok lehallgatására akkor kerülhet sor, ha az állami hálózattól bérel vonalakat.[270]

A lehallgatás, mint a titkos információgyűjtés eszköze a **magyar** jogban is ismert. Hazánkban a rendőrségi törvény (1994. évi XXXIV. tv.) egy teljes fejezetet szentel a titkos információgyűjtésnek. A lehallgatás a magyar jogban (is) bírói engedélyhez kötött, mely alól akkor lehetséges kivétel, ha a bírói engedélyezési eljárás "olyan késedelemmel járna, amely az adott ügyben nyilvánvalóan sértené a bűnüldözés eredményességéhez fűződő érdeket" a nyomozó hatóság vezetője ideiglenes jelleggel, 72 óra időtartamra elrendelheti (Rtv. 71. § (1) - (2) bekezdései). A lehallgatás csak a törvényben taxatíve említett bűncselekmények alapos gyanúja esetén alkalmazható (Rtv. 69. § (1) - (4) bekezdései). Törvényünk a lehallgatás tárgyaként telefonvezetéket vagy "azt helyettesítő távközlési rendszert" (Rtv. 69. § (1) bekezdés c./ pontja) határoz meg. Mivel hazánkban a számítógépes kommunikáció adatátviteli vonalak hiányában leginkább telefonvezetéken bonyolódik, így a telefonvonalakon átvitt számítógépes adatok lehallgatásának törvényi akadálya nem lehet. Viszont egyéb adatátviteli technikák esetében kétely merülhet fel, hogy a telefont "helyettesítő távközlési rendszerek" közé beletartoznak-e a számítógépes információt továbbító adatátviteli vonalak, rádiófrekvenciák és műholdas csatornák. E rendelkezés alapján lehallgatható e technikákkal bonyolódó számítógépes kommunikáció. (Ha a távközlési és informatikai szakemberek véleménye ettől eltérő, akkor a törvényszöveg pontosítása elengedhetetlen.)

A 48/1991. (III. 27.) Korm. rendelet mellékletének XXIII. fejezete tartalmazza a lehallgató eszközök, valamint alkatrészeinek és tartozékainak felsorolását: "I. lehallgató eszköznek minősül bármely elektronikus, mechanikus vagy más eszköz, módszer, "technológia", szoftver, amely az információkhoz egyébként jogosan hozzáférők, illetve a kommunikációban résztvevők tudta nélkül,

---

[270] www.minjust.nl:8080/C__ACTUAL/PERSBER/compcrim.htm - saját fordításban.

titkosan alkalmazható és az alábbi tulajdonságok valamelyikével rendelkezik: .... Digitális vagy analóg információkat tároló és/vagy feldolgozó számítógépekből, számítástechnikai vagy egyéb eszközökből vagy a hozzájuk használható információhordozókon tárolt információk bármilyen módon történő titkos megszerzésére, továbbítására, rögzítésére tervezték, gyártották, vagy erre lényeges átalakítás nélkül felhasználható."

Kényes kérdést vethet fel a különbség az állami-, közcélú szolgáltató (távbeszélő-, mobilrádiótelefon-, valamint személyhívó) - hálózatok és magánhálózatok lehallgatása között. A törvényünk e problémáról nem tesz említést. Arra fel kell készülnie a jogalkotónak, hogy az igen közeli jövőben a magán kábeltársaságok az egyirányú jeltovábbítás (televíziós- és rádióműsorok) mellett megteremtik a kétoldalú kommunikáció technikai feltételeit, így ezek nemsokára interaktív adat- (azaz Internet) és hangátvitelre (telefonszolgáltatásra) is alkalmassá válnak.

Magam a jogbiztonság követelményét szem előtt tartva azon a véleményem vagyok, hogy a törvény nevesítse a lehallgatható hálózatok körét, tehát szerepeljenek a szövegben a magán-, és az állami hálózatok, közcélú szolgáltatóhálózatok elnevezés. Eltérően az osztrák és a német jogi megoldástól, hazánkban a lehallgatás *kivételes* nyomozati eszköz. Tekintetbe véve a számítógéprendszerek és hálózatok elterjedését de lege ferenda meggondolandó lenne: egyfelől a lehallgatás kivételességet feloldani és általános tenni a számítógépes kommunikáció lehallgatását. Szabályai kialakításakor a rendőrségi törvény rendelkezéseiből célszerű kiindulni. Mellőzendő tehát a bűncselekmények taxációja. Másfelől felmerül a tárgyi kényszerintézkedések törvényben megfogalmazott arányossági követelményének expressis verbis kimondása (Be. 105. § (1) bekezdés). Továbbá rendelkezni kellene arról, hogy azon jelentések, feljegyzések, esetleg tárgyak, amelyek a lehallgatás vagy adatrögzítés során keletkeztek és a büntető eljárás szempontjából érdektelenek késedelem nélkül megsemmisítendők legyenek, akár ügyészi felügyelettel.

7. 5. A számítógépes adatok, mint bizonyítékok

A számítógépes adatok többféle módon, formában és technikai eszköz útján keletkezhet és jeleníthető meg a külvilágban. Ez nem kevés nehézséget vet fel, annak bizonyítékként történő értékelésében a büntető eljárás folyamán. Az ET. (95) 13. sz. Ajánlása a problémafelvetés mellett annak megoldásra tesz javaslatot.

"*Az elektronikus bizonyítékokról*

13. El kell ismerni, hogy a hazai büntetőeljárásban és a nemzetközi együttműködéscéljából szükség van az elektronikus bizonyítékok gyűjtésére, fenntartására és bemutatására az épségüket és cáfolhatatlan hitelességüket a legjobban biztosítóformában. Ezért különböző eljárásokat és műszaki módszereket kell kidolgozni az elektronikus bizonyítékok további fejlesztésére, különösen oly módon, ami biztosítja a bizonyítékok államközi kompatibilitását.

A büntetőjogi törvények bizonyítékként felhasznált hagyományos dokumentumokra vonatkozó rendelkezései hasonlóan a számítógépes rendszeren tárolt adatokra is vonatkoznak." [271]

Az angol jogban az 1984-es "Police and Criminal Evidence Act (PACE)" 1988. évi módosításakor kimondják, hogy "a büntető eljárásban a számítógép által kinyomtatott dokumentum bizonyítékként nem használható fel". (PACE 69. §)[272]

E törvényi rendelkezés kapcsán az angol **J.C. Smith** az alábbiakban csoportosítja a számítógép által kinyomtatott adatok bizonyítékként történő értékelésének lehetőségét:

"*a.* Egy számítógépen kinyomtatott dokumentum általában "hallomásnak" (hearsay - innen ered a jogszabály szakirodalomból ismert elnevezése: hearsay-tv.) tekintendő. De bizonyítékként fogadható el, ha pl. egy tisztviselő bizonyos termékről kiállított számlát gépeli be a számítógépbe, majd ennek kinyomtatott példányát mutatják be avégből, hogy azt kézbesítették. Ugyanígy a pénztáros

---

[271] CE Recommendations (95) 13. (v.ö. 204.sz.)

[272] Sir John Smith: Criminal Evidence. London 1995. p.91

begépeli a termékek kódszámát és a pénztárgép szalagján megjelenik, amely majdan tények bizonyítéka lehet.

b. Egy számítógépen kinyomtatott dokumentum lehet maga a tény, amely bizonyításra szorul. Pl. annak igazolására, hogy valóban helyeztek-e el 100 dollárt egy bankszámlára. Ebben ez esetben az maga a tény, hogy a banktisztviselő bebillentyűzte az összeget és azt egy bankszámlára utalta. Ez szorul bizonyításra. Ez az eset nem sorolható a hallomás körébe.

c. Egy számítógépen kinyomtatott dokumentum bizonyíték olyan tényre vonatkozóan, amelyet a számítógép "figyelt meg" és rögzített. Ez nem hallomás, nem egy személy állítása, hanem bizonyíték. Pl. a bank számítógépe rögzíti a berakott bankjegykötegek sorozatszámát, más esetben egy hotel számítógépe rögzíti a vendégek telefonhívásainak idejét és a hívott számot, vagy a szonda rögzíti az alkohol szintet valamint a sebességmérő radar a jármű sebességét."[273]

A büntető eljárás legáltalánosabban nem más, mint megismerési folyamat. A múlt egy eseménye megismerésének folyamata a gyanútól a bizonyosságig. A megismerési folyamat "közhatalmi ténykedés keretében bonyolódik le, egymással szerves kapcsolatban levő, egymásra épülő szakaszokból szerveződik."[274]

Az egységes büntető eljárási folyamat szakaszokra osztását **Király Tibor** szerint "az a tapasztalat és módszer határozza meg, amely szerint az összetett tények megismerése a reájuk vonatkozó részadatok összegyűjtésével kezdődik, amit majd gondolati elemzés és szintézis követ."[275]Más szóval azt is mondhatnánk, hogy a nyomozati szakaszban döntően ténykutatás folyik, míg a bírói szak jellemzője a ténymegállapítás. A tárgyalás során is (pl. tanúvallomás) felbukkanhatnak olyan új tények, amelyeknek a váddá tett cselekménnyel összefüggésbe hozható. E két fázis összefüggése jelenti az egységes megismerési folyamatot. Ez a megismerés mindig *közvetett vagy közvetített megismerés*, hiszen a hatóságok és az érintettek számára a

---

[273] Sir John Smith ... id. mű p(s). 92-93.

[274] Dr. Bócz Endre: "Megismerés" és "bizonyítás" a büntető eljárásban.Megjelent: Emlékkönyv Dr. Cséka Ervin egyetemi tanár születésének 70. és oktatói munkásságának 25. évfordulójára, Szeged 1992. 84.l.

[275] CE Recommendations (95) 13. (v.ö. 204.sz.)

múltbeli eseményre vonatkozó ismereteket más személyek vagy tárgyak közvetítik.

A tanúk, a terhelt, a szakértők lehetnek közvetítők. Ha bizonyíték szűkében van a bíró valamely állítás igazságáról logikai bizonyítás útján győződik meg. Közvetett a megismerés tárgyak (fényképek, helyszínrajzok, video- vagy audiófelvétel stb.) eseteiben is. A közvetett megismerés tárgyait a bírónak általában *közvetlenül* kell észlelnie. A közvetlen vizsgálat követelményét a büntető eljárási törvény az alapelvek közé emeli. "A bíróság - ha e törvény eltérően nem rendelkezik - határozatát a tárgyaláson *közvetlenül* megvizsgált bizonyítékokra alapítja." (Be. 10. § (2) bekezdés, amely az 1998. LXXXVIII. tv. 1. §-a vezet be.) A közvetlenség elvének elemzése során **Tremmel Flórián** felhívja a figyelmet arra, hogy legalább három kérdés megválaszolásával juthatunk el ennek az alapelvnek a jelentéséhez; milyen bizonyítékokat, ki és hogyan vizsgálja a büntetőeljárás folyamán.[276]

Bár a bizonyítékok többféle forrásból meríthetők, ám a bíróságnak törekednie kell az elsődleges ("ősforrású") bizonyítékok felhasználására, szemben a másodlagos, harmadlagos, azaz származékos vagy áttételes bizonyítékokkal, amelyek torzíthatják a bűncselekményre vonatkozó tényeket. **Herke Csongor** megállapítja, hogy az "eredeti bizonyítékok lényege vizsgáló (végső soron az ügydöntő határozatot hozó bíró) között".[277]

A vallomást (nyilatkozatot) tartalmazó okirat sérti a közvetlenség elvét, akkor használható fel, ha "a vallomást tevő nem hallgatható ki, a vallomást megtagadja vagy az okirat tartalma és a vallomás közt ellentét van" (Be. 83. § (3) bekezdés).

A bizonyítóerejű számítógépes adatok közvetlen érzékelése, észlelése, láthatóvá alakítása a kinyomtatott papírlappal vagy a képernyőről készült fényképpel realizálódhat. Az ily módon rögzített adatok a vizualitással válnak közvetlenül észlelhetővé. Ontológiai szempontból viszont másodlagosak, hiszen a számítógép memóriájában vagy egy adathordozón tárolt adat egy papírlap,

---

[276] Tremmel Flórián: Büntető eljárásjog ... id. mű 79.l.
[277] Dr. Herke Csongor: Büntető eljárásjogi alapismeretek. Pécs. 1998. 16.l.

fényképfelvétel közreműködésével jut el a bizonyítékok közé. Természetesen e rögzítés által nem keletkeznek új bizonyítékok, hanem a már meglevő bizonyítékok válnak viszonylagosan tartósan hozzáférhetővé. Némi aggállyal a számítógépes adatokat rögzítő adathordozókat okiratnak tekinthetjük.

A tárgyi bizonyítékok bizonyító ereje sem feltétlen, azokat a bíró más bizonyítékokkal egybevetve, a bizonyítékok szabad mérlegelése körében értékeli. Látható tehát, számítógépes adatokat tartalmazó adathordozó lefoglalásakor biztosítandó hitelesség létfontosságú az eredményes bizonyításhoz.

7. 6. A büntető eljárásban részvevők együttműködési kötelezettsége

Bár legtöbb bűncselekmény felderítéséhez, nyomozásához elengedhetetlen a *sértett* (a károsult) együttműködése, ez a számítógépes környezetben elkövetett jogsértéseknél különös fontosságú.

A nyomozó hatóság és a szakértők számára a sértett igazi remédium, - ha megismerteti a bűncselekménnyel érintett adatok minőségét, jelentőségét, - amennyire lehetséges bemutatja az elektronikus adatfeldolgozási folyamat struktúráját, ellenőrzési mechanizmusait, együtt kutatja a nyomozó hatósággal vagy szakértőkkel a hálózat sebezhető pontjait, - felfedi a számítógépbe- vagy a hálózatba történő belépéshez továbbá file-ok eléréséhez szükséges jelszavakat vagy más azonosító kódokat, - ha szükséges lehetővé teszi az adatforgalom átvizsgálását, rendelkezésre bocsátja az adatfeldolgozási tevékenység dokumentációit, jegyzőkönyveket, - ha történt már korábban a számítógépes adatállományok ellen végrehajtott bármilyen jogsértés, azt is jelzi a nyomozó hatóság felé.

A sértett, mint károsult mellett a terhelt és a tanú kooperációs készsége is elősegíti, elősegítheti az eredményes nyomozást.

A *terhelt* eljárásjogi helyzete kettős, egyfelől a büntető eljárási törvényben biztosított jogok és kötelezettségek alanya (jogi státusz), másfelől a terhelt a leghitelesebb bizonyítékokat szolgáló eszköz (reál státusz). "Következésképpen a

terhelt minden nyilatkozata egyfelől védekezési eszköz /moyen de défense/, másfelől viszont bizonyítási eszköz /moyen d`instruction/."[278]

A terhelt "a legbővebb adatforrás ..... Éspedig döntően ama különös pszichológiai helyzeténél fogva, hogy ő nem - külső - megfigyelője, észlelője volt a bűncselekménynek és fontos tényeinek, hanem átélője, közvetlen végrehajtója."[279]A törvény a terhelt irányába az eljárási jogosultságok mellett számos kötelezettséget ír elő, ezek között szerepel a személyes jelenlétet előíró szabályok a bizonyítási cselekményeknél, a tárgyaláson, továbbá a szakértői vizsgálatok eltűrése. Emellett számos közreműködési kötelezettséget is határoz meg a **magyar büntető-eljárási** törvény.

E kötelezettség tartalma egyfelől meghatározott időben és helyen történő megjelenés, másfelől olyan tevőleges magatartás, amely a keresett tárgy kiadását írja elő (pl. a szemlénél a Be. 84. §, helyszínelésnél a Be. 84/A. §, házkutatásnál a Be. 103. § stb.). Motozás (Be. 104. §) során a bizonyítási eszköz átadását kívánja meg a törvény. A keresett tárgy kiadásának megtagadása rendbírságot nem von maga után, viszont a szemlénél a szemletárgy átadása kikényszeríthető (Be. 84. § (4) bekezdés). A keresett tárgy kiadásának megtagadását követően a hatóság elrendelheti a személyi motozást vagy a házkutatást is. Az inkriminált adathordozók átadásának kötelezettsége a hatályos szabályok alapján megoldható. A számítógépbe vagy hálózatba történő belépéshez, file-ok eléréséhez szükséges együttműködési kötelezettség nem egyértelmű. A "nemo se ipsum accusare potest" elvének megfelelően a terhelt bűnösségének beismerésére nem kötelezhető. Az 1966-ban az Egyesült Nemzetek Közgyűlése által elfogadott *Polgári és politikai jogok nemzetközi egyezségokmánya* megfogalmazza azt az elemi követelményt, hogy a terheltet "ne lehessen kényszeríteni arra, hogy .... beismerje bűnösségét" (14. cikkely g. pont) A kérdés az, amely az előző fejtegetésből is következik, mi tekintendő beismerésének? E körbe nemcsak a bíróság vagy más hatóság előtt tett

---

[278] Dr. Tremmel Flórián: Büntető eljárásjog ... id. mű 128.l.
[279] Dr. Cséka Ervin: A büntető ténymegállapítás elméleti alapjai. Budapest, 1968. 116.l.

beismerő vallomás (confessio rei propria iudicalis et extra iudicalis) tartozik, hanem ennél tágabban értelmezve a terhelő tárgyi bizonyítékok átadása is.

A magyar Be. is lehetővé teszi a terhelt vallomástételének megtagadását, azzal a farizeus megjegyzéssel, hogy ezzel "a védekezésének erről a formájáról lemond" (Be. 87. § (3) bekezdés). A terhelt tehát nem kötelezhető arra, hogy a számítógépbe, hálózatba vagy file-okba történő belépéshez szükséges kódokat, jelszavakat személyesen begépelje vagy az ehhez nélkülözhetetlen információkat közölje valamint a kódolt adatok megfejtéséhez segítséget nyújtson. Ugyanakkor a kódok, jelszavak feltárása folytán előbukkanó bizonyítékok mellett be kell szerezni további alanyi- vagy tárgyi bizonyítékokat Nem kötelezhető továbbá a terhelt a számítógépben- vagy hálózatban kezelt valamint az adathordozón rögzített adat kinyomtatására sem a fenti indokok alapján. Megfontolandó a számítógépbe-, a hálózatba vagy file-okba történő belépéshez nyújtandó terhelti segítséget a büntető eljárási törvényünkben expressis verbis ez együttműködési kötelezettség körébe emelni. Ennek indoka az, hogy a számítógépbe való belépés, vagy valamely adatállományának hozzáférése rendkívül bonyolult biztonsági megoldásokkal lehetetleníthető (bár, abszolút védelem nem létezik), de legalábbis hallatlanul megnehezíthető és ezáltal költségigényessé tehető.

Előfordulhat az, hogy a bűncselekmény tárgyi súlya, és az ezt kifejező kárérték *nincs arányban* pl. a számítógépet illetéktelen hozzáférés ellen védő különböző szintű jelszavak feltörésére, a titkosított dokumentumok visszafejtésére stb. fordított ráfordítással. A nyomozó hatóságnak szakember hiányában a hozzáférés biztosításához esetlegesen hackert kell igénybevenni. Bár beismerésre nem lehet kényszeríteni a terheltet, ezzel ellenkeznék a fenti nemzetközi dokumentummal is, de az inkriminált adatállomány megismertetése a nyomozó hatósággal nem jelent beismerést, hiszen ezen bizonyíték legfeljebb egy láncszem a bizonyítékok láncolatában. Amennyiben a terhelt ezt megtagadja, úgy más tárgyi kényszerintézkedésre pl. (a fentebb említett új szabállyal) a számítógépbe- vagy hálózatba történő belépést megengedő házkutatásra kerülhet sor.

A *tanú* eljárás jogi helyzete szintén kettős. A törvényben biztosított jogok és kötelezettségek alanya és bizonyítékforrás. Amíg a tanú vonatkozásában ezen jogok és kötelezettségek a bizonyíték szolgáltatásának formájára és tartalmára koncentrál, és csak azt hivatott biztosítani, addig a terhelt esetében lévén ő ellene folyik a büntető eljárás, a büntetőjog humanizmust hirdető alapelvének érvényesülése mellett speciálpreventív szempontok is szerepet kaptak. A tanút az eljárás folyamán vallomástételi kötelezettség terheli, amelyet megtagadhat ha annak törvényi lehetősége fennáll. Nem köteles a tanú vallomást tenni, ha a terhelt hozzátartozója, vagy ha magát vagy hozzátartozóját bűncselekmény elkövetésével vádolná kizárólag ebben a kérdésben, továbbá, ha foglalkozásánál vagy közmegbízatásánál fogva titoktartásra kötelezett és vallomásával ezt megsértené, kivétel ha ez alól felmentették (Be. 66. § (1) bekezdés). A vallomástételi kötelezettség teljesítésének vagy megtagadásának lehetősége a büntetőeljárás bármely fázisában releváns. Továbbá a tanú egyes kérdésekre a választ megtagadhatja, míg másokra nyilatkozhat. A vallomástételi kötelezettség megtagadása büntetőjogi jogkövetkezményeket is maga után vonhat pl. hamis tanúzás (Btk. 238. §) bűncselekményének alkalmazhatóságát.

Mindezek előrebocsátását követően leszögezhetjük, hogy a tanú, amennyiben nem forog fenn a vallomását érintő megtagadási ok, köteles kiadni a hatóság számára azokat az információkat, amik a számítógépbe-, hálózatba- vagy bármely file-ba való belépéshez elengedhetetlenek. Ennek szándékos megtagadása már a büntető eljárás sikerének meghiúsítására irányuló törekvésként értékelhető, amely a bűnpártolás bűncselekményének (Btk. 244. §) megállapítására szolgálhat alapul. A vallomástételi, mint legtipikusabb kötelezettség mellett a törvény további tevőleges tevékenységet is megkíván a tanútól. Az egyes eljárási cselekményeknél a keresett tárgy (pl. a szemle Be. 84. §, helyszínelés Be. 84/A. §, házkutatás Be. 103. § stb.), illetőleg a bizonyítási eszköz kiadását (motozás Be. 104. §). Akár a keresett tárgy, akár bizonyítási eszköz átadásának megtagadása rendbírságot von maga után. A nyomozás során keresett adathordozó átadását a tanú nem tagadhatja meg, ha ezt teszi, úgy pénzbírsággal sújtható.

Vajon mindezen közreműködési kötelezettségek közé illeszthető-e a számítógépben kezelt vagy valamely adathordozón tárolt adat kinyomtatásának kötelezettsége is? A **német** Oldenburgi Területi Bíróság egy 1988-ban lefolytatott eljárásában a vállalat egyik könyvelőjét, mint tanút kötelezte arra, hogy a számítógépben tárolt adatot nyomtassa ki.[280] Másik nemzetközi példánkat a **holland** Be. nyújtja azzal, hogy a fenti idevonatkozó szabályokban implicite benne rejlik a tanú együttműködési kötelezettsége.[281]

---

[280] Revue ... p. 352.

[281] www.minjust.nl:8080/C__ACTUAL/PERSBER/compcrim.htm - saját fordításban.

8. A NEMZETKÖZI BÜNTETŐ-JOGTUDOMÁNYT ÉRŐ KIHÍVÁS

Az elektronikus adatátviteli hálózatok nemzetközivé válásával, az adatok áramoltatásával valamint a számítógépes hálózatokba történő belépés lehetőségével a bűncselekményeket elkövetők átléphetik az országhatárokat. Láthattuk, hogy német fiatalok Németországból Egyesült Államokban található adatbázisokat fürkésztek ki. Tehát az elkövetők az egyik országban lépnek be valamely számítógépes hálózatba és billentyűzik be a hamis vagy hamisított adatokat és ez a manipuláció egy másik országban fejti ki hatását, pl. megváltoztatja egy adatállomány tartalmát vagy az ezzel elért vagyoni hasznot vagy valótlanná vált bizonyítékot akár ebben az országban, akár egy harmadik országban használják fel. Ugyanígy a vírus - programok is átléphetik az országhatárokat és egy másik vagy több országban fejtik ki károsító hatásukat. Az adott országban letiltott WEB-oldal (pl. gyűlöletkeltő vagy pornográf tartalma miatt) elérhető egy másik országban, ahol pl. az információáramlás szabadsága miatt nem élnek a tiltás lehetőségével.

A modern információs társadalmak együttműködésre vannak ítélve a bűncselekmények megelőzése és üldözése terén. Az együttműködés két-, illetve ma már jellemzően többoldalú nemzetközi szerződés alapján valósul meg.

Ez utóbbi szerződések közül kiemelkedik a Párizsban, 1957. december 13-án kelt, európai kiadatási egyezmény és két kiegészítő jegyzőkönyve, a Strasbourgban, 1959. április 20-án kelt, a kölcsönös bűnügyi jogsegélyről szóló európai egyezmény és kiegészítő jegyzőkönyve, valamint a Strasbourgban, 1983. március 23-án kelt, az elítélt személyek átszállításáról szóló egyezmény. A magyar Országgyűlés az 26/1993. (IV. 23.) Ogy. Határozatával megerősíti e három megállapodást és a kiegészítő jegyzőkönyveket, a Kormány pedig a megerősítésről szóló okiratot az Európa Tanács Főtitkáránál letétbe helyezi.

A *nemzetközi büntetőjogi együttműködés alapja és realitása* az, hogy az abban részt vevő országok az anyagi jogi, majd eljárásjogi normáikat közelítsék egymáshoz. A büntető anyagi jogi harmonizáció a civiljog harmonizációjához

képest igencsak gyermekcipőben jár. Ennek okai igen sokrétűek lehetnek, úgy tűnik, hogy a büntetőjog más jogágaknál jobban kötődik a nemzeti kultúrához, továbbá egyes országokban eltérő a jogalkalmazási, ezen belül a büntetéskiszabási gyakorlat, hiszen különböző a társadalmak toleranciaszintje, valamint értékrendje, kulturális hagyományai.[282] Bár születnek már egyes kiemelkedően súlyos bűncselekmények üldözésére kötelező ENSZ Közgyűlési Határozatok, valamint nemzetközi szerződések, de ezek száma és az üldözendő bűncselekmények köre csekély. Ma már "a büntetőjog elméletében a belső jog mellett a nemzetközi jogot is a büntetőjog forrásának kell tekinteni."[283]

Ezzel kapcsolatban kell megjegyeznem, hogy az ENSZ konvenciókban lefektetett jogsértések üldözése e határozat aláírásával feltétlenné válik, a "nullum crimen sine lege" szabálya e határozattal ölt testet. A nemzetközi szerződések viszont nem keletkeztetnek közvetlenül ilyen kötelezettséget, üldözésük csak azután lehetséges és kötelező mihelyt a büntető törvénykönyv különös részébe felveszik azokat. Egyes regionális szervezetek további kriminális magatartásokat határoznak meg és javasolnak azokkal szemben közös fellépést. Ezek között az OECD és az Európa Tanács Ajánlásai tartalmaznak az informatikai bűncselekményekre vonatkozó rendelkezéseket.

Az ajánlások jogi természetéről **Kecskés László** megállapítja, hogy "nem tekinthetők jogforrásoknak, de azok ösztönző ereje kétségtelen." [284]

A számítógépes környezetben elkövetett bűncselekmények elleni közös fellépésre az OECD 1985-ben és az Európa Tanács (89) 9. sz. Ajánlása buzdít. Az Európa Tanács - már említett - (95) 13. sz. Ajánlása nemcsak a büntető eljárásjogot érintő kihívásokról szól, hanem a nemzetközi együttműködés egyes kérdéseit is érinti.

---

[282] Dr. Bárd Károly: Európai büntetőpolitika (Tények és kilátások - Tanulmányok Dr. Király Tibor emlékére. Szerkesztette: Dr. Erdei Árpád) Budapest, 1995. 150-151.l.

[283] Dr. Wiener A. Imre: Büntető joghatóság és nemzetközi jog.Állam- és jogtudmány XXXV. 1993/3-4. 211.l.

[284] Dr. Kecskés László: EK jog és jogharmonizáció, Budapest 1995. 119.l.

"A nemzetközi együttműködésről

17. Akkor is biztosítani kell a nyomozás más számítógépes rendszerekre való kiterjesztésének lehetőségét, amennyiben azonnali lépésekre van szükség, ha a rendszer külföldön van. Az állami szuverenitás és a nemzetközi jog megsértésének elkerülése végett ellentmondásmentes jogi alapot kell teremteni a kiterjesztett kutatáshoz és az adat lefoglalásához. Ezért sürgősen meg kell kezdeni a nemzetközi egyezmények aláírásához vezető tárgyalásokat, amelyekben le lesz fektetve, hogy hogyan, mikor és milyen mértékben engedélyezett a házkutatás és a lefoglalás.18. Gyors és megfelelő eljárásokat, valamint kapcsolatrendszereket kell kidolgozni arra, hogy a nyomozó hatóságok hogyan kérhetik a külföldi hatóságokat azonnali adatgyűjtésre. Ebből a célból felkért hatóságot fel kell ruházni a megfelelő hatáskörrel a számítógépes rendszerek átkutatására és az azonnal továbbítandó adatok lefoglalására. A felkért hatóságot fel kell hatalmazni egy adott telekommunikációs eszközön áthaladó adatokat átadására vagy egy adott telekommunikációs eszköz lehallgatására illetve a forrás azonosítására. Erre a célra kiegészítésekkel kell ellátni a már meglevő kölcsönös jogsegély eszközeit."[285]

A tartalmilag egységes kriminalizáció szükségessége vita nélküli, hiszen a hálózatok a határokon túlnőnek. A számítógépes környezetben elkövetett jogsértések büntetendővé nyilvánítása valamennyi országban, vagyis a *double criminality elvének* gyakorlati megvalósítása teremti meg az alapját és realitását a nemzetközi együttműködés már kiérlelt formáinak továbbfejlesztéséhez. Ezen együttműködés büntető anyagi jogi területei hagyományosan az alábbiak:

1. a joghatóság;
2. a kiadatás;
3. a büntető eljárás átengedése;
4. a bűnügyi eljárási jogsegély, valamint egy új lehetőség
5. a "közvetlen belépés" elve.

---

[285] CE Recommendation (89) 9. ..... p(s). 83-91. és Csonka Péter: Council of Europe Activities Related to Information Technology .... id. mű p(s).184-187.

8. 1. A joghatóságról

A büntetőtörvény hatályának meghatározásakor a törvényhozó többféle elvet "az igazság és célszerűség követelte korlátozásokkal egymással összhangba hozni igyekszik" - írta **Kautz Gusztáv** még 1881-ben.[286]A büntető jogszabályok alkalmazhatóságának alapja a kora feudalizmus személyfüggő társadalmi berendezkedése miatt az ún. *személyi vagy honossági elv* (principum personalitatis) érvényre juttatásával kezdődik, majd a feudális széttagoltság megszűntével az ún. *területi elv* (principium territoriale) érvényesül.

Az előbbi elv az uralkodó teljhatalmát szentesíti alattvalóival szemben, az utóbbi elv az állam büntetőigényének érvényesítését jelenti saját állampolgáraival szemben, tehát az állam büntető törvényének alkalmazását rendeli a területén elkövetett valamennyi bűncselekmény elkövetőjével szemben, függetlenül az elkövető állampolgárságától és attól, hogy cselekménye melyik állam érdekei ellen irányul. A területi elv érvénye alól két kivételt fogalmaznak meg korábban, egyik a *területenkívüliség elve*, amely a honossági elvet terjeszti ki, azaz az idegen államban tartózkodó és akkreditált diplomáciai képviselők és ezzel egyenrangú személyek nem a tartózkodási helyük büntető jogszabályai, hanem saját országuk büntető törvényei szerint feleltek.

A másik kivétel az ún. *védelmi elv*, amely szerint egyes államok nemzetközi egyezmény alapján "kivették" saját állampolgáraikat a más országok joghatósága alól. Ezen egyezmények általában a másik ország megszállását, kapitulációját követően születtek. Mivel sem a területi elv, sem a személyi elv maradéktalan érvényesítése nem nyújt kielégítő büntetőjogi védelmet az államok számára, így e két elv konkuráló elemeit igyekeztek az ún. *állami önvédelmi elvben* (principium reale) összebékíteni, ezzel ugyanis út nyílik a büntető törvénykönyv rendelkezéseinek alkalmazására akkor, ha

a. a bűncselekményt az állam területén saját állampolgárai vagy külföldi állampolgár követte el, valamint

---

[286] Dr. Kautz Gusztáv: A magyar büntetőjog tankönyve. Budapest, 1881. 70.l.

b. olyan bűncselekményt valósítottak meg, mely az állam kiemelkedő érdekeit sérti.

Ismert még az ún. *feltétlen büntető hatalom elve* (universalitas elve), amely szerint független az elkövető állampolgárságától és attól, hogy melyik állam területén követte el a bűncselekményt és melyik állam ellen irányul cselekménye felelősségre kell vonni annak az államnak a törvényei alapján, ahol tartózkodik. "Az állami önvédelmi elv gyakorlásának elismerése az ára a szuverén államok együttműködésének."[287]

Az állami önvédelmi elv csak akkor érvényesülhet maradéktalanul, ha az elkövető a hazai hatóságok kezére kerül, akár az elkövető (esetleges) önkéntes jelentkezésével, akár más állam segítségével és ekkor kerül előtérbe a kiadatás intézménye.

8. 2. A kiadatásról

A nemzetközi büntetőjogi együttműködés egyik legfontosabb intézménye, az együttműködés megvalósulása a kiadatás, amely mai fogalmaink szerint csak a XVIII. századtól létezik.[288] Az intézmény lényege az, hogy az egyik állam területén levő személyt, a másik állam kérelmére büntető eljárás lefolytatása vagy büntető ítélet végrehajtása végett átadja a kikérő államnak. Az intézmény általános szabályai néhány évszázad alatt alakulnak ki:

a. a cselekmény a megkereső és a megkeresett állam törvényei szerint büntethető (ne álljon fenn büntethetőséget kizáró vagy megszüntető ok);

b. a kikért személy a cselekményét a megkeresett állam területén követi el (érvényesülhetne a területi elv);

c. az államok saját állampolgáraik kiadatására kötelezettséget nem vállalnak, csak külföldi állampolgár adható ki (aut punire, aut dedere - elv);

d. menedékjogot szerzett személy nem adható ki;

---

[287] Dr. Wiener id. mű 42.l.

[288] Dr. Wiener A. Imre: Jogforrások és jogelvek a nemzetközi büntetőjogban. Állam- és jogtudomány XXXII. kötet 1-4. száma 1990. 16.l.

e. a kiadni kért személy cselekménye res iudicata ne legyen;

f. a kiadott személy csak azért a bűncselekményért vonható felelősségre, amelyre a kiadatási engedély szól (specialitás elve); bár ez utóbbi alól nemzetközi szerződés felmentést adhat;

g. ha más bűncselekmény miatt folyik eljárás a kiadni kért személy ellen a megkeresett államban, a kiadatás foganatosítása elhalasztható az eljárás befejezéséig;

h. szorosan vett politikai vagy ahhoz kötődő bűncselekmények, újabban pénzügyi deliktumok miatt általában nincs helye kiadatásnak.

Az 1957-ben Párizsban kelt az *Európai Kiadatási Egyezmény*, amelyet Magyarország 1993-ban ír alá. Az Egyezmény 1. cikkelye szerint "kiadják egymásnak azokat a személyeket, akik ellen a megkereső fél igazságügyi hatóságai büntetőeljárást folytatnak, vagy akiknek az említett hatóságok a körözését rendelték el büntető ítélet vagy biztonsági intézkedés végrehajtása céljából."

A 2. cikkely (1) bekezdése feltételként szabja, hogy a kiadatási kérelemben feltüntetett cselekmény, mind a megkereső, mind a megkeresett államban büntetendő legyen. Ez a "double criminality" - elvének a törvényi rögzítése. Ez kiegészül egy további kogens feltétellel is, nevezetesen a bűncselekményért legkevesebb egy évi vagy ennél súlyosabb szabadságvesztéssel legyen fenyegetve. E szabályokat hazánkban a nemzetközi egyezmények alapján születő 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről (továbbiakban: NB.) 11. §-nak (2) bekezdése is rögzíti.

Az Egyezmény kimondja továbbá, amennyiben az elítélés a megkereső államban történt a bíró legalább négy hónapi büntetést szabjon ki (ez a "condition of penalty level" - elve). Erről a magyar törvény nem rendelkezik. A kiadatás intézményének egy másik kardinális kérdése a kiadatás megtagadásának lehetősége.

A 6. cikkely szerint a tagállamok bármelyike megtagadhatja saját állampolgára kiadatását. A szerződő államok maguk határozzák meg, kit kell állampolgárnak tekinteni. E rendelkezés az állam és polgára közötti különleges

kapcsolat elismerésén alapul, amely alapján az állampolgár igényt tarthat az állam védelmére.

Ezzel szemben ha valamely szerződő fél úgy dönt, hogy nem adja ki a megkereső fél állampolgárát, akkor - a megkereső fél kérelmére - saját illetékes hatóságai elé kell terjesztenie az ügyet a végett, hogy ha szükségesnek tartják, eljárást folytassanak le. Az eljárás eredményéről a megkereső felet tájékoztatni kell. Ugyanígy megtagadható a kiadatás a 7. cikkely szerint, ha az adott bűncselekményt saját joga szerint egészen vagy részben saját területén vagy ezzel egy tekintet alá eső területen követik el.

A kiadatás megtagadásának még egy lehetőségét nyújtja az egyezmény 8. Cikkelye, amely szerint, ha a kiadni kért személlyel szemben a kérelem tárgyát képező bűncselekmény vagy bűncselekmények miatt eljárás folyik a kiadatás megtagadható.

Magyarország az informatikai bűncselekmények közül a számítógépes csalás (Btk. 300/C. §, amelynek büntetési tétele 3 évvel kezdődik) a bankkártya-hamisítás (Btk. 313/B. §, amelynek büntetési tétele 2 év, ám előkészülete csak pénzbüntetéssel fenyegetett), továbbá a bankkártyával visszaélés (Btk. 313/C. §, amelynek büntetési tétele 2 évtől kezdődik) bűncselekmények esetén van lehetőség nem magyar állampolgár kiadatására (NB. 11-13. §-ai.) Magyar állampolgár kiadatásának csak akkor van helye, ha a kiadni kért személy egyidejűleg más állam polgára is, és állandó lakhelye külföldön van (NB. 13. § (1) bekezdés).

Ezen új típusú bűncselekmények kapcsán több probléma is felvetődik az egyezmény 2. cikkely alkalmazásával kapcsolatban. Vitatott lehet egy - egy cselekmény fogalmának értelmezése és ebből adódóan e magatartás kriminalizálása és szankciójának meghatározása: így a jogosulatlan belépés (a hacking) kriminalizálása nem egységes. Egyes országokban nem büntetendő, más országokban viszont igen, de van, ahol csupán a jogosulatlan belépés szankcionált, míg másutt a belépést követő jogsértések megvalósulásával együtt büntetendő. Ne feledjük azt sem, hogy a szankciók megállapítása nem független egyes országok morális, jogi tradícióitól, továbbá a szankciók rendszerétől. Az Egyezmény 7. cikkelye szerint a kiadatás

megtagadható, ha a bűncselekményt akár részben is a megkeresett állam területén követték el. A **magyar** Btk. területi hatályának meghatározásából következik az, hogy a magyar törvényt kell alkalmazni a belföldön elkövetett bűncselekményre (Btk. 3. § (1) bekezdése). Vagyis a kiadatási kérelem ellenére megtagadható annak az elkövetőnek a kiadatása, aki a számítógép - rendszerbe belépve a gépbe billentyűzi vagy az adathordozóról behívja a hamis vagy hamisított adatot (in - put) és ennek a műveletnek az eredménye egy másik országban realizálódik. Ekkor a megkeresett állam, amelynek területéről indul a bűncselekmény e cikkely szerint megtagadhatja kiadatást jóllehet a bűncselekmény többi eleme, különösen eredménye pl. a vagyoni kár vagy a hamis bizonyíték más ország területén keletkezik.

A kiadatás kérdését tovább nehezíti, ha kettőnél több ország érintett a bűncselekménnyel. Az egyik országban manipulálták a számítógépet, egy másik országban végezte a számítógép műveletet (pl. egy bankszámláról az átutalást) és a harmadik ország területén realizálódott a pénz (pl. az ottani bankszámlán írta jóvá a gép).Ebben a pillanatban - elvileg - akár három ország formálhat jogot az elkövető büntetőjogi felelősségre vonására. A magyar törvény a ugyanazon személy iránt érkezett több kiadatási kérelem eldöntésekor az alábbi körülmények figyelembevételét javasolja: az elkövetés helye (locus delicti), a kiadni kért személy állampolgársága, a megkeresések érkezési sorrendjére, illetve ha a megkeresések különböző bűncselekményekre vonatkoznak, azok súlyára (NB. 17. §).

8. 3. A büntető eljárás átengedéséről

A büntető eljárás felajánlása szintén szoros együttműködést tételez fel, amelynek során az eljárást felajánló állam lemond a joghatóságáról, tehát a megkereső állam ajánlja fel a megkeresett államnak a büntető eljárás lefolytatását. Ezen intézmény működésének összehangolására az *Európai Konvenció a Büntető eljárás átengedéséről* 1972-ben születik. A Konvenció 7. cikkelye hasonlóan a fentiekhez a "kettős büntethetőség" fontosságát emeli ki. A 8. cikkely lehetőséget nyit arra, hogy annak az országnak ajánlják a fel a büntető eljárás lefolytatását, ahol a legfontosabb bizonyítékok fellelhetők. Ennek elfogadása lehetővé teszi a bünte-

tőjogi felelősségre vonást abban az esetben, amikor a bűncselekmény következménye egy másik államban jön létre. E cikkely témánk szempontjából akkor lehet releváns, ha a manipuláció, kalózkodás vagy más bűncselekmények elkövetéséhez használt számítógép a megkeresett állam területén van és ott bizonyítható akár az "elektronikus betörés", akár az adatmanipuláció.

A 30. cikkely (1) bekezdése is visszautal a "kettős büntethetőség" elvére azzal, hogy megköveteli az ugyanolyan bűncselekmény ("the same offence", illetve "les memes faits") fennforgását. Ez a cikkely nyilvánvalóan a tényállások tartalmi azonosságát követeli meg. Ugyanakkor kiélezi a kriminális harmonizáció nehézségeit. A magyar törvény a büntetőeljárást akkor tartja átengedhetőnek, ha azt célszerűnek tartja. Ennek értékelésénél a sértett jogos érdekének mérlegelése mellett főként az elkövető fellelhetőségét tartja szem előtt. A büntetőeljárás lefolytatása akkor engedhető át, ha

a. a Magyarországon tartózkodó terhelt annak az államnak az állampolgára, amelynek részére az eljárás átadása történik vagy abban az államban van állandó lakóhelye, illetve a szokásos tartózkodási helye,

b. a terhelt az eljárás során külföldön tartózkodik, kiadatásnak nincs helye, kiadatását megtagadták, vagy kiadatási kérelem előterjesztésére nem kerül sor (NB. 37. § (2) bekezdés). Ez a felsorolás tehát nem taxatív, amiből az következik, hogy a Konvenció 8. cikkelyében említett eljárás átengedését jelentő lehetőség azon országok számára, - ahol a legfontosabb bizonyítékok találhatók - nem kizárt.

Külföldi állam igazságügyi hatósága előtt folyó büntető eljárás a hatóság megkeresésére akkor vehető át, ha a terhelt magyar állampolgár vagy Magyarországra bevándorolt nem magyar állampolgár. (NB. 43. §)

8. 4. A szűkebb értelmű bűnügyi jogsegélyről

Bűnügyi jogsegély keretében a megkereső állam eljárási cselekmény elvégzésére igényt tarthat a megkeresés tárgyául szolgáló büntető ügyben.

Az 1959-ben születetik *Kölcsönös Bűnügyi Jogsegélyről szóló Európai Egyezmény* Strasbourgban, amelyhez Magyarország 1993-ban csatlakozik.

Ezen egyezmény 2. cikkely b./ pontja kimondja azt, hogy a jogsegély megtagadható, ha a kérelem teljesítése sértheti a megkeresett ország "lényeges érdekeit". Mivel a megkeresett állam területén működő számítógéprendszerek- és hálózatok kezelhetnek a megkeresett állam és/vagy polgárai számára érzékeny adatokat is, így a megkeresés megtagadása ezen ügyekben realitás.

A **magyar** törvény valamennyi jogsegélyi formát érintően fogalmazza meg a megkeresés megtagadásának feltételeit: így nem teljesíthető a megkeresés, ha az csorbítja a Magyar Köztársaság felségjogait, veszélyezteti biztonságát, sérti közrendjét (NB. 2. § (1) bekezdés).

Az Egyezmény 3. cikkelye szerint a jogsegélykérelem irányulhat bizonyíték beszerzése vagy bizonyítékul szolgáló tárgyak, ügyiratok, okiratok megküldése céljából. A citált hazai törvény kissé hosszúra sikeredett felsorolásban említi az eljárási jogsegély lehetőségeit: így különösen nyomozati cselekmények teljesítése, a bizonyítási eszközök felkutatása, a terhelt és a tanú kihallgatása, a szakértő meghallgatása, szemle, házkutatás, motozás, lefoglalás, hazánkon keresztül történő átszállítás, a bűnüggyel összefüggő iratok, tárgyak megküldése, kézbesítése, a külföldön büntetőeljárás alá vont magyar állampolgárra vonatkozó és a bűnügyi nyilvántartásban szereplő adatok ideiglenes átadása (NB. 61. § (2) bekezdése). Elegendőnek tűnt volna a magyar büntető-eljárási törvényben szabályozott intézményekre történő hivatkozás mellett egyes speciális jogsegélyi módot kiemelni.

Az informatikai bűncselekmények nyomozása során a bizonyíték megszerzésének többirányú problémái e körben is jelentkeznek, így a lehallgatás alkalmazhatóságának vagy az adathordozók tartalma megismerésének országonként eltérő szabályaiban. Ez utóbbi esetben ismételten fel kell hívni a figyelmet arra, hogy egy - egy adathordozón általában nemcsak az inkriminált adatok lelhetők fel, hanem más, esetleg érzékeny adatok is. Az ET. (89) 9. sz. Ajánlást előkészítő bizottság a joggyakorlat hiányát észlelve, igyekszik olyan speciális szempontokra utalni, amelyek a számítógépes környezetben elkövetett bűncselekmények körében

jogsegély iránti megkeresési kérelem tartalma és végrehajtása kapcsán napvilágra kerülhetnek. Az *ET. (89) 9. sz. Ajánlása* az alábbi:

A. A jogsegély *tartalmára* vonatkozóan:

a. a megkeresési kérelemben meg kell jelölni az inkriminált rendszer vagy programok lehető legpontosabb leírását,

b. a számítógépes rendszer lehallgatása iránti kérelem csak akkor bocsátható ki, ha más eljárási cselekmény nem alkalmazható,

c. utalni kell arra, hogy a megkeresésben írt eljárási cselekményeket a megkereső ország hatóságai engedélyezik,

d. meg kell jelölni a keresendő adatok lehető legpontosabb részleteit.

B. A jogsegély *végrehajtásának* feltételei kapcsán adott ajánlások:

a. a megkeresett fél hatóságai bizonyos adatok kiadását megtagadhatják jellegük miatt;

b. a megkereső fél hatóságainak a lehető leghamarabb időn belül meg kell semmisítenie vagy helyreállítania azokat az adatokat, amelyek a büntető eljárást nem érintik, a megsemmisítésről szóló jelentés a megkeresett fél számára megküldendő;

c. a nyomozási cselekmény végrehajtását követően a megkeresett fél törvényei vagy gyakorlata alapján tájékoztatni köteles a számítógéprendszer tulajdonosát, üzemeltetőjét, kezelőjét arról, hogy nyomozási cselekmény folyt ellene, továbbá az összegyűjtött adatokról.

d. a segélynyújtási kérelemben és a megkeresett fél által megadott segélyben megjelölt célon kívül, az adatokat más célra nem használhatják a megkereső fél hatóságai, kivéve a megkeresett fél beleegyezését.[289] A magyar törvény nagyfokú rugalmasságról téve tanúbizonyságot, megengedi azt, hogy a magyar eljárási

---

[289] 289. CE Recommendations (89) 9. sz. ..... p(s).91-94.

szabályok mellett a megkereső ország által ajánlott eljárásmódokat is lehet alkalmazni akkor, ha ez nem összeegyezhetetlen a hazai jogrendszer alapelveivel (NB. 64. § (1) bekezdés).

8. 5. A "közvetlen belépés" elvéről

Az országokat összekötő számítógépes hálózatokban folyó adatáramlás felveti azt a kényes kérdést is, hogy a nyomozó hatóságok más országok adatbázisait elérhetik-e vagy az ott tárolt adatokat felhasználhatják a nyomozás céljára pl. bizonyítási kísérletnél. Nem kevésbé problematikus az a kérdés, hogy az "elektronikus betörőket" forró dróton követve átléphetnek-e, "belehallgathatnak-e" idegen országok rendszereibe? E problémakörben összemérhetetlen érvek feszülnek egymásnak, hiszen egyfelől a hagyományos bűnügyi jogsegély igénybevételéhez nélkülözhetetlen, de hosszadalmas procedúra a nyomozás eredményességét hiúsíthatja meg, másfelől a "közvetlen belépés" a nemzeti számítástechnikai rendszerekbe az államok féltve őrzött területi szuverenitását csorbítja, emellett a számítástechnikai rendszerekben kezelt érzékeny információk napvilágra kerülése sértheti az érintett állam vagy egyes szerveinek érdekét.

Az ET. (89) 9. sz. Ajánlásának megfogalmazásakor az Előkészítő Bizottság megfontolásra érdemesnek véli a "közvetlen belépés" alkalmazhatóságát nagyon szigorú feltételek meglétekor, ilyennek kell tekinteni: - a "közvetlen belépés" során csak olyan intézkedések jöhetnek számításba, amelyek érintetlenül hagyják az adatok status quo-ját, tehát azok nem változtathatók meg stb. - az adatokat csak az állam hozzájárulásával lehet használni, - csak súlyos jogsértés esetén lehetséges a "közvetlen belépés", - a hagyományos bűnügyi jogsegély érvényesítéséhez szükséges idő veszélyezteti a nyomozás sikerességét, - tájékoztatási kötelesség a hazai nyomozó hatóság felé stb. A Bizottság summázatul megállapítja, hogy jelenleg az idő nem érett meg ezen elv gyakorlati alkalmazhatóságához, mivel ez összeegyezhetetlen az állami szuveneritás tiszteletben tartásával.[290] Bár a "közvetlen

---

[290] 290. CE Recommandations (89) 9. sz. ..... p(s) 86-88.

belépés" elvének megvalósulása csupán ad futuram tekintve realitás, de nem eltékozolt idő alaptételeinek tisztázása.

9. NÉHÁNY GONDOLAT A BŰNMEGELŐZÉSÉRŐL

Az informatikai bűnözés a számítástechnikai és a telekommunikációs technika fejlődésével jelent meg és válik egyre számottevőbbé.

Az emberi gondolkodás, az emberi jogok kiteljesedése, a bűnügyi tudományok fejlődése, és eredményei mára elvitathatatlanná teszik az olasz Cesare Beccaria megállapítását, miszerint a "bűncselekményeket jobb megelőzni, mint büntetni."[291] A bűnmegelőzés komplex kérdéskörében az informatikai bűnözés megelőzésének *általános szintjén* ugyanazon eszközök, intézmények alkalmazhatók vagy folyamatában alkalmaznak, mint bármely más bűncselekményfajták esetében.

A társadalom erkölcsi fejlődésének és anyagi jólétének fokozása, mint generális célkitűzés helyessége elvitathatatlan. E helyes célok elérése nemcsak a gazdaság felemelkedésének függvénye, hanem az elosztás prioritásának meghatározásában is rejlik. Hatásuk eredményessége hosszabb távon érzékelhető. Ezzel együtt a társadalmi együttélés normáinak megismertetése, elsajátítása, a morális értékek tisztelete is egyre fontosabb.

A társadalom anyagi javakban történő gazdagodásával egyre többen juthatnak számítógéphez, más technikai eszközökhöz, Internet-eléréshez, amely az informatikai bűncselekmények elkövetéséhez nélkülözhetetlen. Ugyanígy az oktatási rendszer minden szintjén növekvő szerepet kap a számítástechnika elsajátítása, amely az ismeretet, a tudást nyújtja. Természetesen szó nincs arról, hogy akár a számítógéphez, mint eszközhöz illetőleg a számítástechnikai ismeretekhez való közelebb kerülés helyessége megkérdőjelezhető.

A bűnmegelőzés *különös szintjén* az informatikai bűnözés ellen ható nem jogi és jogi, ezen belül büntetőjogi lehetőségek összegezhetők.

Az ET. (89) 9. sz. Ajánlás az alábbi "nem büntető jellegű prevenciós eszközöket" javasolja:

---

[291] Cesare Beccaria: Bűntett és büntetés. Budapest, 1967. 134.l.

"- a számítógép használói által hozott önkéntes biztonsági intézkedéseket;
- kötelező előírásokat a biztonsági intézkedések betartására bizonyos kényes területeken;
- a szervezeten belül, a vezető vagy a rangidős adminisztrátor által hozott vagy az ügyvitelben rögzített előírásokat a biztonság, illetve a bűncselekmény megelőzése érdekében;
- az információs technológiai ipar biztonsági intézkedéseinek kidolgozását, magyarázatát és ismertetését;
- fejlesztést, támogatást a számítógép etika terjesztésében, valamennyi társadalmi szektor, különösen az oktatás, a hivatásos társulások és a média által;
- az adatfeldolgozó iparban a hivatalos szabványok fejlesztését;
- a sértett együttműködésének előmozdítását a számítógépes bűncselekmény feljelentésében;
- a nyomozó, a vád és az igazságszolgáltatási rendszerek személyzetének oktatását és kiképzését."[292]

I. Az elektronikus adatfeldolgozás és a telekommunikáció elleni támadások megelőzésének különös szintjén az első és legfontosabb lépése e tevékenységek fizikai biztonságának és jogi környezetének kialakítása. Mivel a számítástechnika gyors ütemben fejlődik, ennek következtében a biztonság megoldások folyamatos fejlesztése követelmény.

1. Az elektronikus adatfeldolgozó- és a telekommunikációs rendszerek fizikai biztonsága nem egyszerűen annak működését (áramkimaradás-, tűz-, villám elleni védekezést), valamint a vagyonvédelmet foglalja magában, hanem az illetéktelen hozzáférés és rácsatlakozás kizárását is. Ennek számos egymásra épülő módszere létezik, így

---

[292] CE Recommendations (89) 9. sz. ..... p(s). 94-98.

- a számítógépes helyiség védelme (beléptető rendszerekkel, riasztókkal, zárakkal stb.)
- a hardver védelme (a számítógép riasztóra kapcsolása, a gép bekapcsolásakor jelszó kérése stb.)
- az elektronikus adatfeldolgozás- és telekommunikáció folyamatának védelme a jogosulatlan hozzáféréstől (a gépbekapcsolásától, a hálózatra történő bejelentkezésen át az operációs rendszerhez való hozzáférésig felhasználói nevek és kódok kérése, a hozzáférések naplózása stb.),
- adat- és szoftver védelem (adatfájlok titkosítása, a szoftverek másolásvédelme, hologrammal való ellátása stb.)

A számítástechnikai és telekommunikációs rendszerek abszolút védelme nem valósítható meg. A védelemnek olyan fokúnak kell lenni, hogy a bűncselekmény elkövetőjének sem költség-, sem időráfordításban ne érje meg a rendszer elleni támadás.

2. Az elektronikus adatfeldolgozás és telekommunikáció folyamatának jogi szabályozására szolgáló számtalan jogszabály felöleli e tevékenység fizikai biztosítását és jogi, ügyviteli rendjének meghatározását. (pl. a rendszerhez hozzáférők körének meghatározása, az adatfeldolgozás- és továbbítás rendjének tisztázása, az adathordozók tárolására és más tevékenységre vonatkozó rendelkezések). Érintik e kört a számítógépes adatokra is vonatkoztatható adat- és titokvédelmi jogszabályok.

3. Az informatikai rendszerek legsebezhetőbb pontja az e tevékenységet végző ember.

Az elektronikus adatfeldolgozás bármely fázisában résztvevő személyek szakmai ismeretén túl erkölcsi tartásuk, anyagiasságuk és más személyes tulajdonságuk megismerése is a munkakör betöltésének szempontja lehet. Figyelemre méltó problémának tartom a személyes tulajdonságok megismerésének,

feltérképezhetőségének egzaktságát és összeegyezhetőségét a személyiségi jogok tiszteletben tartásával.

II. A bűnmegelőzési stratégia - bármennyire is szeretnénk - nem nélkülözheti a büntetőjogi reakció lehetőségét.

1. Az informatikai bűncselekmények büntetőjogi eszközei közül a büntetni rendelt informatikai bűncselekmények aggálymentes definiálásának követelményét kell kiemelnem.

A törvényhozó ezáltal jeleníti meg a társadalomra veszélyes és büntetni rendelt magatartásokat, amelyek tanúsításáért szankció alkalmazására számíthat. Ehhez kellő segítséget nyújt az ET. (89) 9. sz. Ajánlása. Különösen az opciós listán szereplő cselekményfajták áttekintését tartom alapvetőnek.

Ugyanilyen fontos a büntető-eljárási törvény (tárgyi) kényszerintézkedésekre vonatkozó szabályrendszerének átvizsgálása, amelyhez viszont az ET. (95) 13. sz. Ajánlása ad nélkülözhetetlen útmutatást. A hatályos Btk.-ból még hiányoznak az informatikai bűncselekmények teljes körű megfogalmazása. A büntetőjogi tényállások megalkotása a kormány és a parlament felelőssége és kötelessége.

2. A büntetőjogi szankciók megalkotásával a törvényhozó kifejezésre juttatja rosszallását, azaz kinyilvánítja, hogy az adott magatartás tanúsítása milyen joghátránnyal fenyegetett.

a. Ha az informatikai bűncselekmények súlyszerinti fokozatait tekintjük, akkor a bűncselekmények adott körében a legkorábbi veszélyeztetés az "elektronikus betörés".

Magam ezt vétségként fogalmaznám meg, így az "elektronikus betörés" révén okozható csalás, adatrongálás-, módosítás, adatkifürkészés stb. már bűntetti alakzatként szerepelne.

Hollandiában, Finnországban a jogosulatlan belépés alapesetéért hat hónapi szabadságvesztés, Olaszországban három évig terjedő szabadságvesztés jár.

b. A Btk. 300/C. §-ban megfogalmazott számítógépes csalás büntetési tétele általában követi az európai jogalkotás trendjét: a német és svájci Btk.-ban öt évig terjedő, az olasz Btk.-ban három évig terjedő és az osztrák Btk.-ban 25 ezer schilling feletti kárértéknél három évig terjedő szabadságvesztés jár. A szankció tehát beleillik az európai jogalkotás trendjébe, a tényállás szövegezése viszont nem.

3. Beccaria fogalmazza meg az utókor számára azt a bölcs gondolatot, hogy a "bűnözésnek legerősebb fékje nem a büntetések kegyetlensége, hanem azok elmaradhatatlansága."[293]

Vajh' valamennyi bűncselekmény elkövetője, így minden informatikai bűncselekmény elkövetője is a büntető igazságszolgáltatás látókörébe kerülhetne. E körben látenciával számolnunk kell. A bűncselekmény elkövetése - más bűncselekményekhez képest - könnyebben leleplezhető, gyorsabb és a pénzintézetek ellenérdekeltsége a bűncselekmények felfedésében is realitás.

4. Az informatikai bűncselekmények számtalan és váratlan elkövetési módja arra kellene, hogy ösztönözze az elektronikus adatfeldolgozásban-, átvitelben érdekelt személyeket, szervezeteket, hogy a bűncselekmény elkövetését megkönnyítő jogi-, technikai, valamint az emberi mulasztásból eredő hiányosságokat, az Internet aktuális megtévesztő, avagy durva, uszító, pornográf stb. WEB-oldalainak ismeretét megosszák egymással.

Erre alkalmat adna a korábbi évek szignalizációs gyakorlata vagy más a tapasztalatcserének lehetőséget nyitó fórum megteremtése.

5. A büntetés kiszabásánál és az intézkedés alkalmazásánál messzemenőn figyelembe kell venni azt a körülményt, hogy olyan fiatalkorúak, fiatal-felnőttek ellen indult büntető eljárás, akik első ízben állnak bíróságok elé, akiknél a

---

[293] Beccaria: .... id. mű 99.l.

kíváncsiságuk, kivagyiságuk motívuma került előtérbe, akiknél nem rögzült az antiszociális beállítottság. Velük szemben elsősorban a speciálpreventív szempontok érvényesítését vélem helyesnek.

6. Az informatikai bűncselekmények felderítése, bizonyítása magasfoku számítástechnikai ismereteket követel, amelynek elérése a jogalkalmazás számára is elsődleges cél.

Az ideális állapot az lenne, ha a jogalkalmazók számítástechnikai tudásban, az Internet ismerésében magasabb színvonalon állnának.

III. A bűnmegelőzés egyedi szintje

A kriminálprofilaxis ezen szintjén a konkrét bűncselekmények megelőzésének lehetőségei vizsgálandók.

A *számítógépes csalás* elkövetésének számtalan lehetősége miatt a bűnmegelőzés különös szintjén feltüntetett biztonságtechnikai eljárások alkalmazása az elsődleges. Hiszen az elektronikus adatfeldolgozást- és átvitelt jogtalan haszonszerzés végett befolyásolhatják, manipulálhatják távközlési vonal át közvetetten, az adatfeldolgozást végző számítógép billentyűzetéről adatok begépelésével közvetlenül. Vagy másféle csoportosításban: a számítógép nemcsak eszköze, hanem célja is lehet a bűncselekmény elkövetésének. Látható, hogy egyedi megelőzési módszerek kiemelése nem vezet eredményre.

A büntetőjogi eszközök között ehelyütt is kiemelem a Btk. 300/C. §-nak felülvizsgálatának szükségességét.

A *bankkártyával visszaélés* bűncselekményének visszaszorításáért egyaránt sokat tehetnek a kártyakibocsátók, a bankok, valamint a kártyabirtokosok.

Mivel a bankkártyaforgalom dinamikája töretlen a kártyakibocsátók felelőssége mindenekelőtt a bankkártyák biztonságának fokozása. A bankkártyák hamisítása ellen a meglevő biztonsági technikák mellett a chippel ellátott és a biometrikus jegyek (ujjlenyomat, retinamintázat stb.) felismerésére alkalmassá tett

kártyáké a jövő. A bankok a kártyabirtokosok adatainak védelméért, az ellopott vagy elveszett kártyákat feltüntető "fekete-lista" gyorsabb frissítéséért, közzétételéért, a bankjegykiadó automaták biztonságos(abb) működéséért stb. felelősek. Speciális megoldásokkal (pl. a kártyabirtokos készpénzfelvételi, fizetési szokásainak figyelésével, kiemelkedő összegek átutalásakor rákérdezéssel is) védhetik a kártyaforgalom biztonságát, a hamis kártyák és tranzakciók kiszűrését.

A bankkártyatulajdonosoknak fokozott figyelmet kell fordítaniuk bankkártyáikra. A négyjegyű azonosító kódot (az ún. PIN-kódot) ne hordják táskáikba, más irataikkal, mivel ez is a zsebtolvajok célpontja. Alkalmanként kisebb összegeket emeljenek le kártyaszámláikról. Ehhez a bankok együttműködésére is szükség van, azaz a bankoknak mérsékelniük kell tranzakciós díjaikat.

A bankautomatánál ügyeljünk arra, hogy ne fürkészhessék ki az azonosító (PIN-) kódot, az automata billentyűzete ne legyen átlátszó anyaggal leragasztva.

Vásárláskor pedig ne engedjünk kártyáinkat elvinni a pénztártól, ne közöljük a pénztárossal vagy mással kódszámainkat, illetve ha be kell ütnünk kódszámunkat, azt ne figyelhesse ki senki.

ÖSSZEFOGLALÁS ÉS EPILÓGUS

Mivel Magyarország gazdasági elmaradottsága és politikai kényszerpályára taszítottsága folytán az elektronikai, így a számítástechnika fejlődésében is "megkésett", ami az elszalasztott előnyök mellett annyi pozitívummal járt, hogy később kerülünk szembe a számítógépes környezetben elkövetett bűncselekménnyel is. Ezen időben megismerhetjük más országok jogi, ezen belül büntetőjogi válaszait.

A számítógépes környezetben elkövetett bűncselekmények kodifikálásának első fázisán már túl vagyunk és nagyon rövid időn belül a második szakaszba kell lépnünk, amikor a következő törvényhozási feladatokat kell véghezvinni:

1. Kriminalizálni a *számítógépes rendszerekbe történő jogosulatlan belépést*, amely az elektronikus adatfeldolgozás integritását töri meg. De lege ferenda a szabályozás szubszidiárius lenne, azaz ha ez a jogosulatlan belépés ("elektronikus betörés") nem valósítana meg más, az alább ismertetett bűncselekményt.

2. A *számítógépes csalás* szövegének újrafogalmazása elkerülhetetlen, bár rendszerbeli helye is aggályos. Ahogy fentebb utalok rá az 1978. évi IV. Btk. 300/C. § (1) bekezdésében "keverednek" a csalás és a rongálás elemei. Nehézséget vett fel az (1) bekezdés magatartás-bűncselekmény mellett a (2) bekezdésben írt eredmény-bűncselekmény kísérletének megállapítása. Törölni kell a (3) bekezdés részletezést teremtő tényállását.

Szem előtt tartva az ET. (89) 9. sz. Ajánlását és a nyolcvanas- kilencvenes évek jogalkotási trendjét szem előtt tartva kívánatos: egyfelől a számítógépes csalás tényállását a vagyon elleni bűncselekmények közé beemelni, másfelől visszatérni a Pusztai László által adott definícióhoz, amelyet alapul vett az 1994-ben az Országgyűlés elé beterjesztett Kormányjavaslat is. A Javaslat ekképp fogalmazza meg a tényállást: "aki jogtalan haszonszerzés végett valamely számítógépes adatfeldolgozás eredményét a program megváltoztatásával, törléssel, téves vagy hiányos adatok betáplálásával, illetve egyéb, meg nem engedett műveletek végzésével

jogellenesen befolyásolja, és ezzel kárt okoz, bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő."

3. A számítógépes csalás jelenleg hatályos szövegének kitisztázásával egyidejűleg a *számítógépes adatok és programok elleni támadások* büntetőjogi üldözésének lehetőségét szükséges kialakítani. Ebben a rongálás tényállásának struktúráját követve a jogellenes adat- és programváltoztatással előidézendő károkozás lenne büntetendő.

4. A *mikroelektronikai félvezetők* (a chipek) utánzásának, átvételének tilalma más szerepel a hatályos magyar Btk.-ban. Az ET. (89) 9. sz. Ajánláshoz igazodna a számítógép chipjeinek jogosulatlan felhasználásának, forgalombahozatalának büntetni rendeltsége.

5. Mivel szinte valamennyi bűncselekmény nyomozásánál, bizonyításánál felmerülhet (tárgyi) *kényszerintézkedések* alkalmazására számítógépes környezetben szükséges a Be. néhány rendelkezésének módosítása. Az ET. (95) 13. sz. Ajánlásával kerülne összhangba az 1973. évi I. törvény 103. § (1) bekezdésének olyan módosítása, amely a *házkutatás* helyei (tárgyai) közé felvenné az "elektronikus adatfeldolgozó rendszert". Ez a nevesítés azért fontos, mivel ez, mint rendszer nem lokalizálható egy helyiségben. A bűncselekmény nyomozása során az elektronikus adatok *lefoglalására* csak akkor kerülhet sor, ha ezen inkriminált adatoktól megfosztják a számítógép használóját, mint gyanúsítottat.

A megfosztás megvalósulhat a számítógép elvitelével, a memóriaegység kiszerelésével és az adatok kimásolásával. Ez utóbbi során a számítógépből először kimásolni, majd törölni kell az adatokat. Ennek során biztosítani kell az adatok tartalmi eredetiségét. Ugyanakkor az adatok vagy programok törlésénél fel kell hívni a figyelmet arra, hogy ez a nyomozati cselekmény nagyobb kárt idéz elő, mint a bűncselekmény tárgyi súlya. A számítógépes adatfeldolgozás titkossága a legkülönfélébb belépési és más kódokkal, jelszókkal védett folyamat, tevékenység.

Egy-egy biztonsági megoldás úgy is kialakítható, hogy a kódok, jelszók megfejtése egyrészt lényegesen nagyobb energiát emészt fel, mint a bűncselekmény tárgyi súlya. Másrészt a kódok, jelszavak próbálgatásával elinduló vírus- vagy más program teszi tönkre az inkriminált adatállományokat.

Ez a szempont a büntető eljárásban *résztvevők együttműködési kötelezettségének* újragondolására ösztönöz. Magam - vitát előrevetítve - a terhelti kötelezettségek közé emelném a számítógép rendszerekbe való belépést lehetővé tevő kódok, jelszavak kiadását.

6. A *nemzetközi bűnügyi együttműködés* fokozása a számítógépes hálózatok nemzetközivé fejlődésével e bűncselekmény csoportban nélkülözhetetlen.

A gyermekpornográfia bűncselekményével összefüggésben elengedhetetlen a világ valamennyi országának összefogására, amely tilalmazást jelent.

Más bűncselekmény esetében a hagyományos intézmények, rendelkezések nyitva állnak.

Ne feledjük, hogy a bűnügyi jogsegély igénybevételének egyik általános feltétele a "kettős büntethetőség" (double criminality) megteremtése. Már ez a tény is ösztönzően kell, hogy hasson a hazai törvényhozásra.

Hitünket az informatikai bűncselekmények elleni sikeres küzdelemben erősítse **Irk Albert** a pécsi egyetem büntetőjogi tanszékének alapítójának és majd' három évtizeden át kiváló tanszékvezetőjének gondolatai: "A békés társadalom és a vele szembe helyezkedő gonosztevő között örökös küzdelem van. Mindazt, mit a tudomány és a technika nyújt, egyik a másik ellen igyekszik csatasorba állítani..... A gonosztevő van elöl, azt elérni igyekszik a társadalom. A küzdelem folyton tartó,

melyből csak egy harmadik kerül ki véglegesen győztesen és ez az emberi előrehaladás."[294]

[294] Irk Albert tanulmányai a büntetőjog és a nemzetközi büntetőjog köréből (Összegyűjtötték: tisztelői, barátai, tanítványai) Pécs, 1928. 57.l.

DR. NAGY, ZOLTÁN: DIE INFORMATISCHE SRAFTATEN

I. Die Forschungsaufgabe und ihre Vorgeschichte

1. In dem letzten Drittel des zwanzigsten Jahrhunderts *bedeutet* die Bewertung und die Kriminalisierung des Mißbrauchs von den Technicken der Datenverarbeitung und - Übertragung sehr verschieden sein.

Was das *Inhalt* angeht, beeinträchtigen oder gefährden diese Verhaltensweisen einerseits traditionellen Werte oder Interessen, doch die Qualifizierung dieser Verhaltensweisen ist nicht jederzeit nach den traditionellen Tatbeständen der Strafgesetzbücher möglich. Andererseits werden die durch die Informationstechnologie geschaffene neue Werte (die Sicherheit der elektronischen Datenverarbeitung, der E-mail, der E-business) Ziele von Mißbräuche, die Bedingungen zum strafrechtlichen Schutz dessen muß man jetzt schaffen.

Das im Strafrecht elementare Prinzip von nullum crimen sine lege erfordert die Modifizierung von schon existierenden Tatbeständen oder die Erschaffung von neuen Verbrechenstypen.

Novum ist die Bildung des strafrechtlichen Schutzes der immateriellen Güter für *dies materielle Strafrechtswissenschaft.*

Die Straftaten neuer Art lassen auch *die Rechtswissenschaft des Strafverfahrens* nicht unberührt. Die Ermittlung und die Beweisführung beansprucht auch neue Methoden und vorbereitete Detektive.

Mit der Erscheinung von Computernetzen bedeuten die informatischen Verbrechen einen besonderen Muster für die Notwendigkeit der *internationalen Zussammenarbeit von Kriminalbehörden.* Ohne die Erstärkung von diesem letzten ist die erfolgreiche Verfolgung von diesen Straftaten unvorstellbar.

All diese haben einen solchen Problemkreis vorgeführt, der mein Interesse erweckt und meine Forschungstätigkeit inspiriert hat.

Mit der Erschöpfung der rechtlichen und technischen Sicherheit von den

Computersystemen beschäftigt sich die Wissenschaft der Informatik, so *halte ich* die Benennung von informatischen Rechtsverletzungen beziehungsweise (wegen ihren späteren Kriminalisierung) Verbrechen *für zweckmäßig.*

2. *Zielsetzung* der Forschung ist die tiefgehende Prüfung von Verbrechensarten, die man im Umfeld von Computern anstellt, im Kreis vom System der Kriminalwissenschaften, mit der Verwendung der Methoden dieser Wissenschaften.

Für die Nachforschung ist die *Komplexität* charakteristisch, sie prüft also die kriminologische Fragen dieser Straftaten, die Analyse der Problemen des materiellen Strafrechtes und des Strafverfahrens sowie die Möglichkeiten der internationalen Zussammenarbeit von Kriminalbehörden.

Wegen der Komplexität dieser Dissertation erfolgt es sich, daß sie sich die Lösung von *zwei Forschungasufgaben* unternimmt. Einerseits werde ich die Strafgesetzgebung ausländischer Staaten für die informatischen Mißbräuche vorstellen. Andererseits werde ich für die heimische Gesetzgebung de lege ferenda Vorschläge angeben, beziehungsweise werde ich die Kritik der heimischen de lege lata Regelung geben.

3. Die *Methode* der Forschung konzentriert sich in erster Linie auf die Rechtsvergleichung. Ich werde die Rechtssetzungs-, Rechtsanwendungs- und rechtliterarischen Fesstellungen von mehr als zwanzig Ländern vorstellen.

Gewisshaft habe ich mich danach bestrebt, daß ich die Charakteristik der Rechtsetzung von solchen Ländern zitiere, die die rechtlichen Traditionen betrachtet zu uns Nahe stehen. Obwohl auch die Rechtspraktikum der Englisch sprechenden Länder bietet uns benutzbare Elemente.

Ich werde noch zwei Empfehlungen des Europarates stark betonen: "Die Computer abhängige Straftaten" (Computer-related Crime) von 1990 und "Strafverfahrensrechtliche Probleme bezüglich der Informationstechnologie" (Concerning Problems of Criminal Procedure Law Connected With Information Technology) von 1995.

Die Bedeutung der ersten Empfehlung steht darin, daß sie das erste Mal die Delikte definiert, die zweite gibt Lösungsvorschläge für a posteriori vorgekommenen Strafverfahrens-problemen.

Obwohl diese Empfehlungen für Ungarn nicht obligatorisch sind, doch in diesem Kreis zeigen sie in der schweren Harmonisierung des europäischen Strafrechts vorwärts.

Wir müssen noch vor dem Auge halten, daß die Grundlage der internationalen Zusammenarbeit die "double criminality", also das Prinzip der zweisamen Strafbarkeit ist.

Die *Struktur* der Dissertation betrachtet kann man sie in fünf größeren Einheiten aufteilen.

II. Zusammenfassung von den neuen wissenschaftlichen Ergebnissen

5. Kriminologische Aspekte

Dieser Teil der Dissertation ist eher wie eine Abschreibung. Ich bestrebe mich für die umfangreiche Aufarbetung und Systematisierung von dem Fachliteratur, das zur Zeit der Dissertation zugänglich ist.

5.1 Die umfangreiche kriminologische Vorstellung der informatischen Verbrechen wird durch die Latenz, die im Kreis dieser Straftäten sehr typisch ist, erschwert. In der Aufdeckung der elektronischen Angriffen (Computermanipulationen, Mißbrauch von Kreditkarten usw.) haben die Finanzinstituten leider gegensätzlichen Bestrebungen wie die Kriminalbehörden.

Aber ebenso undurchschaubar ist die Kopie und der Verkauf von Softwares ohne Erlaubnis.

5.2 Die Mißbräuche im Umfeld von Computern sind gleichaltrig mit dem Erscheinen der Computern in der Zivilsphere. Schon am Ende der fünfzigen Jahren wurden Manipulationen um Eigennutz begangen, dieser Ziel kann auch heute als typisch betrachtet werden.

Schadenwert der Straftäten, die man mit Computer eines Vermögens wegen begangen hat, kann den Schadenwert des auf traditioneller Art eines Vermögens wegen begangenen Straftates weit übertreffen.

Auch die unberechtigte Verwendung von Softwares, die verbotene Kopierung von Mikrochips sowie die Erscheinung von Pornograf-Aufnahmen in der Internet können durch unbefugten Eigennutz motiviert werden.

In diesem Kapitel kann man über die allgemein bekannten Mustern der internationellen Fachliteratur lesen, über den Fall der sog. Equity Funding, über den Rifkin Fall und anderen.

5.3 Auch die Absicht der unberechtigten Auskundung von Staats-, Dienst-, Geschäfts- und Bankgeheimnis, von geschützten Personalangaben ist ein typischer Motiv.

5.4 Mit dem Ausbau von Computernetze wurde der Kreis der mit Computer begehbaren Verbrechen erweitert. Diese können die verschiedensten sein; neuer Schauplatz der Verbrechen gegen die Gemeinruhe (Anreizung gegen die Gesellschaft, Verbreitung von Schreckensnachrichten, Bedrohung mit Gemeingefahr usw.) ist der Internet, aber es wird auch Drogen Popularität gemacht, man kann alle Wissen über die Herstellung von Bomben finden, über die "Dienstleistungen" der Maffia, von extremistischen Organisationen usw.

5.5 Von den Arten des Computermißbrauchs ist eine der gefährlichsten der *hacking* (elektronisches Einbrechen). Die hackers finden die die Kode, die den Eintritt des Users sichern, heraus und brechen dadurch die Integrität, die Sicherheit des Computersystems.

Die unberechtigte Auskundung der Daten kann der pubertären Neugier sowie das Ziel des Erwerbens von Geschäfts- oder Staatsgeheimnis führen. In dieser Dissertation können Sie unter anderen über (west)deutschen Jugendlichen lesen, die sich zur Dienst der KGB begeben haben, um die meist geschützten Systeme der

USA aufzubrechen in der zweiten Hälfte der achtziger Jahren. Aber Sie können auch über den Mitnick - und Poulsen-Fall lesen.

Mit dem Ausbau von Computernetzen (Extranet, Intranet, Internet) kann jeder, jederzeit von jedem Ort die elektronische Datenbestände in Gefahr bringen.

5.6 Weitere Charakteristik der im Computerumfeld begangenen Straftäten ist das Tempo des Begehens, das ihr nachforschung bedeutend erschwert.

6. Antworte auf die Herausforderungen, die die Strafpolitik und die Strafwissenschaft erreichen

6.1 Mit den Fesstellungen von hervorragenden heimischen Autoren wie Pál Angyal , Károly Bárd , Imre Békés, Ervin Hacker, Ákos Farkas, Ferenc Finkey, Géza Finszter, József Földvári, Kálmán Györgyi, Albert Irk, Ferenc Irk, Imre Kertész, Miklós Lévai, Kálmán Merényi, Ferenc Nagy, László Pusztai, Géza Tokaji, Mihály Tóth, Imre A. Wiener, und die ausländischen wie Karl Binding, Raymond Gassin, Michael Gemignani, Otto Harro, Henrik Kaspersen, Franz von List, Peter Schick, Gabriele Schmölzer, Ulrich Sieber, Martin Wasik und anderen möchte ich die Komplexität der Herausforderungen, die die materielle Rechtswissenschaft erreichen,darstellen, und werde die darauf gebende Antwortmöglichkeiten suchen. Danaben bestrebe ich mich auf die Vorstellung von meinem eigenen Ansichtspunkt.

6.2 Pfilcht der jeglichen Verwaltung ist die Organisierung des Kampfes gegen das Verbrechen, die Gewährleistung der dayu nötigen Bedingungen. Dies kann in Einklang mit den allgemeinen politischen Zielsetzungen geschehen. Das Kenntnis- und Begriffsystem der Strafrechtwissenschaft, ihre innere Logik, ihre Gesetzlichkeiten - als Filter – zwingen die kriminalpolitische Entschlüsse der Verwaltung in rechtlichen Rahmen. Über den Begriff der kriminalpolitik können wir verschiedene Meinungen in der ungarischen Fachliteratur lesen. Laut einiger Autoren umarmt die Kriminalpolitik einen breiteren Kreis, als die Strafpolitik, da

die erste auch auf die Problemen, die mit der Abweisung zusammenhänge, eine Achtung geben muß. Andere haben die Meinung, daß wir den Begriff der Kriminalpolitik nur wegen der Egsaktheit der Forschung auf die Strafrechtbildung und Rechtanwendung einschränken.

Auch diese Dissertation will sich dazu anschließen. Es ist unbesttreitbar, daß der Wirkungskreis der Kriminalpolitik über die Rahmen der Gerichstpflege reicht.

Die Gestaltung der nationalen Strafpolitik wird heutzutage immer stärker und nicht grundlos von dem internationalen Recht beeinflußt. Grundlage der Annäherung der nationalen Rechtsysteme, darin des Strafrechtes ist die materielle, produktionelle und technische Zusammenbundenheit der Welt. Dieser objektive Prozess der Annäherung wird auch durch eine andere traurige Erscheinung verstärkt, nämlich das immer breiter gewordene internationale Verbrechen. Dies führt zu der Vertiefung der straftätigen Zusammenwirkung.

Die Rückkehr unseres Landes unter die entwickelte, demokratische Länder Europa erfordert von uns, daß wir diejenigen internationalen Normen annehmen und sie als einen Teil des inneren Rechtes anerkennen, die auch diese Länder annehmen und den sie folgen.

Die Internationale Vereinbarungsurkunde der Bürgerschaftlichen und Politischen Rechte, die auropäische Menschenrechtliche Konvention, die Soziale Charta und anderen internationalen dokumente sowie die Beschlüsse des Menschenrechtlichen Gerichts bilden einen organischen Teil des ungarischen materiellen und immaterielen Strafrechtes.

6.3 In einem Dokument des Europarates von 1990 wird eine sog. Minimale und eine sog. Optionale Liste erstellt, wo das erste Mal die zur Kriminalisierung vorgeschlagene Tätigkeiten definiert wurden. In der Empfehlung von 1995 gibt Vorschläge auf die Lösung von Problemen, die sich während des Strafverfahrens gebildet haben. Indirekt wirkt noch die Datenschutz - Vereinbarung (Nr. 108) des Europarates von 1981 auf diesem Gebiet, dies war die Grundlage zur Ausabeitung der Teilregelungen des Datenschutz - Gesetzes Nr. LXIII von 1992 in Ungarn.

6.4 Unter diejenigen, als bestrafend erklärten Verhaltensweisen, um die Ordnung des gesellschaftlichen Zusammenlebens, die Reproduktion der Gesellschaft, ihre harmonische Entwicklung zu gewährleisten, sind auch solche zu finden, die seit Jahrzehnten, oder schützen die grundlegende Normen, Interssen und Werte des gesellschaftlichen Zusammenlebens (wie das Leben, die körperliche Unverletzbarkeit, Gesundheit, die Ehre, das Eigentum, die Geschlechtsfreiheit, die politische Macht usw.) Gleichzeitig damit machen die gesellschaftliche, wirtschaftliche und politische und/oder technologische Veränderungen die Kriminalisierung von neuen Verhaltensweisen beziehungsweise die Löschung oder leichteren Bestrafung von schon existiernden Straftaten notwendig. Zu diesem letzten Kreis gehören auch die Mißbräuche, gerechtswidrige Verhaltensweisen, die man im Computerumfeld begeht und die durch ihren speziellen Eigenschaften für die Strafrechtwissenschaft eine große Herausforderung bedeuten.

6.5 Eigenschaft der informatischen Sraftaten ist, daß der Gegenstand der Tätigkeit die unsichtbaren informatischen Daten und die körperlosen elektronischen Impulse sind. Die Daten können nach ihren Inhalt gesehen sehr vielfaltig sein, ihre Funktione sind breit. Sie können Vermögenswert, Person gebundenen Daten, Text, Zeichung oder Tabellen als Grund einer Rechtswissenschaftlichen Bewertung usw. Darstellen.

Die Daten kann man unberechtigt ausforschen oder modifizieren: teilweise oder völlig löschen, überschreiben, ersetzen usw. Diese Einmischungen werden das Inhalt der Daten, das man erscheinen lassen möchte, verändern. Diese Modifikation kann in Geld ausdruckbaren Schäden verursachen, kann die Zivilsphere der bezüglichen Person verletzen oder einen Nahcteil anderer Art für die Person bedeuten, die man mit den Daten in Beziehung stellen kann. Unbefugte Löschung eines Datenbestandes oder die Behinderung der elektronischen Datenverarbeitung auf einer anderen Art kann die Telekommunikation, anderen Kommunikationsarten, Produktionstätigkeit, finanzielle Prozesse lähmen, es ist fähig zur Schaffung von

haßerregenden, pornografen, Schreckennachricht ausdrücken ausdruckbaren Schäden verursachen, kann die Zivilsphere der bezüglichen Person verletzen oder einen Nahcteil anderer Art für die Person bedeuten, die man mit den Daten in Beziehung stellen kann. Unbefugte Löschung eines Datenbestandes oder die Behinderung der elektronischen Datenverarbeitung auf einer anderen Art kann die Telekommunikation, anderen Kommunikationsarten, Produktionstätigkeit, finanzielle Prozesse lähmen, es ist fähig zur Schaffung von haßerregenden, pornografen, Schreckennachricht ausdrückenden Texte, Zeichungen etc. Mit der unberechtigten Sammlung Verwendung und Weiterleitung der Daten können die Interessen der berührten Person verletzt werden. Ein Computersoftware ist eine logische Reihevon Algorytmen, die mit Daten gewisse Operationen vollenden kann. Die Ausarbeitung, Schaffung von solchen Programmen ist eine immaterielle Tätigkeit.

Das Strafrecht muß also den Schutz der Daten, als Träger vielschichtigen Informationen und der Daten, als eines Systems, also Programs lösen.

6.6 Abgesehen von den letzten Jahrzehnten dieses Jahrhunderts konzentrierte sich die Strafrechtwissenschaft auf den Rechtschutz von physisch existierenden Gegenständen, die man zum Besitzer oder berechtigten Eingentümer binden kann.

Die Regelungen sanktionieren die ungerechte Wegnahme, Beschädigung usw. dieser Gegenstände auf verschiedenen Weise. Diese Sachen stellen die durch das Strafrecht geschützte materielle Verhältnisse für die Aussenwelt dar.

Im Laufe der Rechtsentwicklung werden im allgemeinen in der ganzen Welt, annähernd mit gleichem Inhalt die untere Angriffe gegen das Vermögen:

a) Unberechtigte Wegnahme des Vermögens von einem anderen (Stehlen, Räubern, Erpressung),
b) Unberechtigtes Umgehen mit berechtigt übernommenen Vermögen eines anderen (Unterschlagung),
c) Übergabe des eigenen Vermögens durch Täuschung (Betrug),

d) Beschädigung, Vernichtung (beschäddigung) des Vermögens eines anderen und... wir könnten die Reihe noch lange fortsetzen.

6.7 Den Wirkungskreis des Strafrechtes muß man also neben den Schutz des in der Aussenwelt verkörperten Objekte auch auf die mit menschlichen Augen nicht erblickbaren, über keinen physischen Existenz verfügenden, nur in gewissen Umgebung über eine Bedeutung verfügenden elektronischen Impulse ausbreiten. In dem ausländischen Fachliteratur kann man immer öfter über die Notwendigkeit der strafrechtlichen Paradigmenwechsel lesen, da man das traditionelle Prinzip des strafrechtlichen Schutzes von Gegenständen, die über physischen Existenz verfügen und mit Augen erfassbar sind, und deren Institutionen für den Schutz der elektronischen Daten nicht völlig adaptierbar ist.

Mein Ansichtspunkt in disem ist das folgende:

1. Der über physischen Existenz verfügende Sachgegenstand ist an einem Inhaber oder gerechtigen Besutzer gebunden, durch den Begehen eines traditionellen Straftates werden all seine Teilrechte (z.B.: Besitz, Gebrauch) gleichzeitig beeinträchtigt oder gefährdet.

Im Falle der immateriellen Güter kann man das Eigentum nicht realisieren.

All die Rechte betreffen nicht nur das Datensubjekt, sondern sie teilen sich mehrfach auf, (Datensubjekt, Dateninhaber usw.) und die einzelnen Elemente all dieser Rechte stehen nicht selten gegenüber oder sie konkurrieren sogar miteinander.

2. Die Rechte zu der Information sind weder inhaltlich, noch formell gleich mit dem jeden anderen ausschliesenden Rechtd es Besitzers oder berechtigten Inhabers der Vermögensgegenstände. Wenn es so wäre, würde das prinzip des freien Flusses der Information beeinträchtigt.

Während des rechtlichen Schutzes der Computerdaten muß man den ausserordentlich sensitiven Gleichgewicht zwischen dem Datensubjekt und – Besitzer oder Sammler bilden, sowie zwischen dem gesellschaftlichen Interesse des freien Flusses der Information. Zu diesem Ziel muß man auch das Mittelsystem eds

Strafrechtes unterwerfen.

3. Die elektronischen Daten haben nur in bestimmter Umgebung, zur bestimmten Zeit eine Bedeutung, dadurch einen Wert für das Datensubjekt, den Datensammler oder für anderen Informationsbesitzer. Aus dieser Ugebung kann man die Informationen nur wegen gesellschaftliches Interesse ausheben oder benutzen, weiterleiten. Andererseits verletzt die gesetzwidrige Auskundung, die Durchführung von Operationen, Weiterleitung, Anwendung der Informationen in erster Linie das Interesse der betreffenden Person, ferner aber auch das der ganzen Gesellschaft. Mit der Beachtung der obigen Ansichte muß man verschiedene Regelungen zustande bringen.

6.8 Ein ungeheuer wichtiges gesellschaftlich-wirtschaftliches Interesse ist die Sicherheit, der Schutz des Prozesses der immer breiter und bedeutender gewordenen elektronischen Datenverarbeitung und Datenübertragung, der technischen Bedingung, der dort verarbeiteten Daten, die Gewährleistung der Ungestörenheit, also die Sicherstellung der Integrität des Systems der elektronischen Datenverarbeitung und Datenübertragung.

Dies bildet – meiner Meinung nach – den Rechtgegenstand des im Computerunfeld begangenen Verbrechens. Den vielfaltigen Funktionen des elektronischen Datenverarbeitungsystems folgend verletzt ein Angriff gegen dieses System im allgemeinen auch andere gesellschaftlichen Interessen, deshalb können die informatischen Verbrechen meistens mit zweisamen Rechtsgegenstand charakterisiert werden: z.B. im Falle eines Computerbetruges werden neben der Integrität, der Sicherheit der elektronischen Datenverarbeitung auch die Vermögensverhältnisse verletzt, oder im Falle eines Verhaltens, das die persönlichen Daten verletzt, wird auch das Interesse zur Geheimhaltung der persönlichen Daten beeinträchtigt.

Ein gemeinsamer Rechtsgegenstand kann den selbstständigen Kapitel der informatischen Straftaten oder binnen eines Kapitels einen Subkapitel also Titel fundieren.

Nach schneller Übersicht der internationalen Rechtsbildung habe ich die unteren Lösungen gefunden:

- Es gibt Länder, die die zu diesem Kreis gehörenden Straftaten in einem Strauß gesammelt in einem selbstständigen Gesetz (z.B. in England wurde 1990 der Computer Misuse Act herausgegeben) oder in einem Kapitel der Besonderen Verordnungen (z.B. in Frankreich im III. Kapitel des Besonderen Teiles) vorstellen.
- In anderen Ländern werden diese Straftaten neben den traditionellen Rechtsgegenständen verletzenden Sachbeständen (z.B. in Deutschland, Österreich usw.) oder als ein Fall deren (wie in Sweden oder Finnland etc.) bestimmen.

Meiner Meinung nach kommen diese Delikte kurzfristig in die traditionelle Besonderen Teil Struktur, nach längerer Zeit werden sie aber einen selbstständigen Kapitel davon bilden.

Grund dafür ist einerseits das, daß ihr gemeinsamer Rechtsgegenstand definierbar ist, andererseits sind die Begehensverhalten dieser Verbrechen gleich (z.B. Datenveränderung, Eingabe von falschen oder mangelnden Daten, Programm-Manipulationen).

Wir können hier an die Geschichte der kodifikation der Verkehrsstraftaten.

Meiner Ansicht nach stehen die elektronische Daten im Fokus der informatischen Straftaten, die also zur gleichen Zeit das Mittel oder das Ziel dieser Verbrechen sein können. Dementsprechend tipisiere ich die informatische Rechtsverletzungen nach den folgenden:

1. Das elektronische Datei als Mittel der Straftaten:

a) Direktes Mittel der Datenmanipulation, die man mit der Absicht

- des Eigennutzes (z.B. Computerbetrug, Mißbrauch der Kreditkarte, Vorstellung einer gefälschten WEB-Seite an der Internet);
- der Fälschung;
- der Schadenstiftung (z.B. Virus-Programme);

- der Sabotage (z.B. Störung von Kommunikationssysteme) begeht.

b) Direktes Mittel: Schöpfung und Erscheinung von haßerregenden-, pornografen oder anderen gesetzwidrigen Datenbeständen an der Internet etc.

2. Elektrisches Datei, als Ziel des Begehens vom Straftat:

- unbefugte Auskundung von persönlichen, besonders persönlichen Daten, gemeinnützigen Daten, sowie rechtlich geschützten Geheimnissen, als zur elektronischen Datenverarbeitung bestimmten Daten, diese für unbefugten Personen zugänglich zu machen usw.
- verbotenes Abhören der elektronischen Kommunikation (e-mail, e-business)
- Mißbrauch von Softwares (Kopie, Anwendung, verbotenes Handel von von Urheberrecht geschütttzten Programmen etc.)

Der unbefugte Eintritt (der Hacking) in die Computernetze ist auch eine Rechtsverletzung eigener Art, da es auch ein Vorgeschehnis der obigen sein kann.

8. Einige Verbrechensarten

8.1 Zur rechtlichen Qualifizierung der im Computerumfeld begangenen Mißbräuche müssen wir die spezielle Charakter, technische Grundlage der einzelnen Verhaltensweisen kennenlernen. Aufgrund dessen kann man sich entscheiden, ob das bestimmte Geschehnis in den Rahmen eines abstrakten Sachbestandes einpasst oder nicht.

Falls wir mit den bekannten Methoden der Rechtsauslegung die Folgerung betreffen, daß es nicht möglich ist, dann ist – nach dem garantiellen Prinzip der nullum crimen sine lege – die Bestimmung von neuen Sachbeständen nötig, es besteht aber die Gefahr der Verdoppelung der Sachbeständen.

Vorgänglich muß man nur soviel feststellen, daß sich die ungarische Gesetzgebung mit der Kriminalisierung einiger Geschehnisse in Verspätung befindet, z.B. der Hacking, die unbefugte Datenveränderung), andererseits wäre in Bezug auf das Urheberrecht eher die Dekriminalisierung empfohlenswert.

8.2 Aufgrund der Verletzung des gültigen Urheber- und Nachbarrechts sind heute in Ungarn mehrmals Zehntausend Computernutzer potentielle Straftäter.

Diese Verordnung, die auf ploitischen Druck zur Welt gekommen ist, ist nicht einzuhalten. Es ist in der Wirklichkeit unmöglich, alle Computer, die in dem Land benutzt werden, gleichzeitig zu kontrollieren, um herauszufinden, wer benutzt an seiner Maschine Softwares aus illegaler Quelle.

Das Halten der irreal hochen, mit Extraprofit belasteten Preise der Softwares sind auch eine Überlegung wert, da entscheidungsgemäß das beeinflußt die Rechtsverletzungen bezüglich der Softwares. Die unberechtigte Benutzung der Computerprogramme, ihre Kopie, Verkauf usw. sind typisch zivilrechtlichen Rechtsverletzungen.

Die strafrechtliche Strengheit muß gegen die geschäftlichen Kopierer und Verkäufer der Computerprogramme in Geltung treten. Diese verbotene Tätigkeiten verletzen stark die finanziellen und geschäftlichen Interessen der Rechtinhaber. Der Kampf sollte auf diesen Kreis konzentriert werden.

Neben diesen kritischen Bemerkungen stehen leider nicht die fachlichen Argumente.

8.3 Das elektronische Einbrechen in die Speicher des Computers oder in ein Netz durch den Computer, als unberechtigter Eintritt ist schon an sich selbst rechtverletzend, doch die wirkliche Gefahr steckt in dem Verhalten nach dem Eintritt. So können Daten modifiziert, gelöscht werden, man kann Geldüberweisungen durchführen, Viren oder andere zerstörerische Programme eingeben, Datenbestände kopiert, Kommunikation abgehört werden usw.

Aufgrund dessen scheint die Erklärung dieses Tates als selbstständiger Straftat mit einer subsidiaren Charakter begründet, ähnlich zu der holländischen Lösung, die ich in der Dissertation vorstelle.

Der elektronische Einbrecher kann nur dann zur Verantwortung ziehen, wenn er mit diesem Tat nicht einen anderen -- unten ausgefalteten – Tat begeht. Der

unbefugte Eintritt würde de lege ferenda – seinen Gewicht betrachtet – die Verstoßform nicht übertreffen.

Die finnische Lösung ist unterschiedlich, sie werde ich in der Dissertation auch vorstellen.

8.4 Die Qualifizierung des Betruges durch Computer ist bis heute nicht nur in Ungarn sondern auch in der Fachliteratur anderen Länder bestritten.

Die Streit geht um die Rolle des Computers als Mittel, beziehungsweise darum, ob es dabei um die Täuschung von einer natürlichen Person geht.

In den Strafgesetzbüchern der west-europäischen Länder steht der Betrug durch Computer im allgemeinen neben dem Sachbestand des traditionellen Betruges oder als ein Fall dessen (Schweden, Finnland) oder in selbstständigen Sachbestand (Deutschland, Österreich, Dänemark).

In Ungarn wurde die Bestrafung des Betruges durch Computer seit 1994 verordnet, in Bezug dessen gebe ich mein Bedenken an.

Bedenken bezüglich des § 300/A des ungarischen SGB-es:

a) Die Verordnung, die Umschreibung des Sachbestandes gibt einen Grund zur Erklärungsstreit. Der Gesetzvorschlag hebte das Ziel aus und schaffte dadurch einen Begriff, der mit dem des traditionellen Betruges konkurriert. Das angenommene Gesetz erklärt die Beeinflussung der elektronischen Datenverarbeitung als Begehensverhalten strafbar.
b) Benennung des Sachbestandes ist "Betrug durch Computer", aber in seinem Text sind nicht nur Elemente des Betruges sondern auch Elemente der Beschädigung zu finden. Dadurch entsteht einWiderspruch zwischen dem Titel und dem Inhalt. Diese Problem könnte dadurch gelöst werden, daß man neben dem Betrug durch Computer später auch den intellektuellen Angriff gegen die Datenverarbeitung regelt. Diese letzte Verbrechenskategorie ist "die Verhinderung der elektronischen Datenverarbeitung und- Übertragung".
c) Der (3) Absatz des § 300/A bestraft die unberechtigte Beeinflussung einer speziellen Form der elektronischen Datenverarbeitung. Die Benutzung der

gefälschten gemeinnützigen Telefonkarten oder SIM-Karten kann man als eingebende (input) Datenmanipulation verstehen, ebenso wie die unberechtigte Veränderung der Daten an dem Chip des Mobilfunkgeräten.

d) Weitere Rechtsanwendungsproblemen entstehen in Bezug auf die falschen, gefälschten Telefonkarten: Die Fälschung der Karte ist ein Tat, der gegen dem (1)Absatz des § 300/A verstoßt, ihre Anwendung aber verstoßt gegen dem (3) Absatz des gleichen Gesetzes.

Auch der "fallosen" Fall, der im (3) Absatz geregelt ist, löscht meine Bedenken nicht, die wegen der Methode der Regelung des Betruges durch den Computer und wegen des Platzes dieses Verbrechens im System entstanden sind. Meiner Meinung nach zeigen die Fälschung der Telefonkarten und die Vermehrung der analogen Mobilfunkgeräten klar und deutlich die wirkliche Bedeutung dieser Taten, und zwar die Datenmanipulation zum Zile des ungerechtigten Eigennutzes.

All diesen werde ich de lege ferenda Vorschläge zur Veränderung der regelung geben, wo sich mehrere Lösungen geben:

- Ausser Kraft Setzung des (3) Absatzes des § 300/A des SGB. Die Betonung von jeglicher Computernetzen ist unwichtig.
- Man sollte zu dem Vorschlag von 1994 zurückkehren.
- Man könnte den Sachbestand des traditionellen Betruges (§ 326 des SGB) mit einer ausbreitenden Erklärung für die Qualifizierung des Betruges durch Computer entsprechend machen. (Wie es auch die skandinavischen Länder machen.) Vorteil diesen letzten ist die Verschwindung der durch die Rechtsanwendung erscheinenden Unsicherheit, die bei der Abgrenzung des Betruges durch Computer und des traditionellen Betruges entsteht, wenn der Computer bei dem Begehen des Verbrechens eine Rolle spielt.

Man kann die Kriminalisierung der durchgeführten Manipulationen an "einfachen Computersysteme" (wie Telefonkarten, Taxiuhren usw.) um Eigennutz aufwerfen (siehe schwedische Regelung). Meiner Ansicht nach würde es in diesem Kreis eine Überregelung und viel Unsicherheit bedeuten, was könnte als "einfaches

Computersystem“ betrachtet werden, da ein taxative Auflistung im Gesetz wohl nicht anzugeben ist.

8.5 Die unberechtigte Datenveränderung, wie ein intellektueller Angriff gegen den Prozess der elektronischen Datenverarbeitung.

Die verursachten Schaden können in verschiedenen Formen erscheinen: Löschung von Datenbeständen teilweise oder vollständig, Formattieren der Festplatte, Lähmung oder Überlastung der elektronischen Datenverarbeitungstätigkeit usw. Die Ersetzung der Datenbeständenist auch eine kostbare Tätigkeit.

Der Trend der rechtlichen Regelung von Ländern, wo ich meine Untersuchungen durchgeführt habe, zeigen, daß die unbeerchtigte Datenveränderung ein selbstständiger (Österreich,, die Schweiz) oder ein subsidiärer Straftat ist (wie in Italien). Die unberechtigte Datenveränderung wurde typisch neben den Sachbestand der Beschädigung eingepasst.

Ein neuer Sachbestand in dem ungarischen Strafgesetzbuch würde den Unterschied klar zeigen, der in dem gültigen § 300/A eingemischt wurde.

9. Antworte auf die Herausforderungen, die die Wissenschaft des Strafverfahrens betrofen haben. Bei der Analyse der Herausforderungen, die die Rechtswissenschaft des Strafverfahrens und der internationellen Strafrechtswissenschaft erreicht haben, habe ich mit den Gedanken von hervorragenden Autoren wie Pál Angyal , Károly Bárd, Endre Bócz, Ervin Cséka, Géza Katona, Gusztáv Kautz, Imre Kertész, Tibor Király, Flórián Tremmel, Imre A. Wiener und im weiteren Wolfgang Bär, Ulrich Sieber, Sir John Smith und anderen die Antworte auf die Herausforderungen, die die Wissenschaft des Strafverfahrens betroffen haben, gesucht.

Da es zwischen den strafenden materiellen und Verfahrensrechtwissenschaft eine enge Beziehung gibt, betrifft eine Veränderung im materiellen Recht selbstverständlich auch das Verfahrensrecht.

Die “Körperlosigkeit“ und “Unsichtbarkeit“ der Computerdaten, wie

elektronischen Impulse bedeutet nicht nur für die materiellen Rechtswissenschaft sondern auch für die Verfahrensrechtwissenschaft zahlreiche Problemen. In diesem Teil untersucht die Dissertation die unteren Themenkreisen:

a) Hausdurchsuchung,
b) Beschlagnahme,
c) Abhörung;
d) Computerdaten als Beweise,
e) Pflicht der Beschuldigten und der Zeugen zur Zusammenwirkung.

9.1 Unter den Zwangsverfahren, die die menschliche und bürgerliche Rechte verletzen und im Gesetz geregelt sind, wäre bei der Hausdurchsuchung die Angabe des "elektronischen Datenverarbeitungsystems" unter den Gegnständen der Hausdurchsuchung mit der Empfehlung des Europarates von 1995 – de lege ferenda – in Einklang. Diese Benennung wäre deshalb wichtig, weil man das elektronischen Datenverarbeitungs- und Übertragungssystem im Raum nicht lokalisierbar ist.

9.2 Bei der Analyse der Inbeschlagnahme ist eine der ersten Fragen, ob man während der Untersuchung eine "Datei" oder einen "Datenträger " in Beschlag genommen hat. In Beschlag nehmen kann man nur materiellen Beweismittel, es kann also nur ein Datenträger sein, das kann sich erst aber erfolgen, wenn der inbeschlagnehmende Gegenstand vomBesitz des Beschuldigten verschwindet. Das kann nur verwirklicht werden, wenn der inkriminisierte Datenbestand nach der Kopierung auf den Datenträger von der Memorie des Rechners gelöscht wird. Die Sicherstellung der Authentität dieser Daten ist aus Garantiellen ansicht sowohl für die Kriminalbehörden als auch für die Betreffenden wichtig.

Meiner Ansicht nach könnte die Veränderung des ungarischen Strafverfahrensgesetzes bezüglich der Beschlagnahme von Computerdaten notwendig werden. Mit dieser Suplementum ist auch der Einbau von Garantien unentbehrlich. De lege ferenda wäre nur die Festsetzung von den Bedingungen der Visualisierung der zur Rechtsfindung bei der Sache selbst unverlassbaren Daten

notwendig. Im weiteren sollte man noch sichern, daß Daten, die das Intersse von Privatpersonen, Wirtscchaftsorganen und anderen verletzen könnten, nicht zur Tageslicht geraten. Begründet wäre die Vorschrift, daß die Abspielung von in Beschlag genommenen Datenträgern nur in der Anwesenheit eiens Staatsanwalt möglich wird.

DR. NAGY, ZOLTÁN: THE INFORMATION-TECHNOLOGY CRIME

I. The subject of research and previous history

1. In the last third of the twentieth century the evaluation and criminalization of electronic data-processing and -transmission is a challenge for criminal studies.

The abuse of data-processing and -transmission may appear in various *forms*, due to their diverse functions.

These ways of behaviour hurt or threat traditional values and interests on one hand in their *content* - though classifying them is not always possible concerning traditional jurisdiction. On the other hand, new values brought forth by informational technology (electronic data-processing, e-mail, the safety of e-trading) turn out to be the aim of abuse; the conditions of criminal liability have to be laid down.

The basic principle of criminal law: nullum crimen sine lege demands the stipulation or alteration of new kinds of criminal deeds. It is a novum for *material criminal law* to establish the measures for the defence of immaterial goods.

The new sorts of crimes do not leave *penal law jurisdiction* untouched either.

Investigation and argumentation also reqiuire new methodology and qualified detectives.

Computer-related crimes show the necessity of *mutual assistence* definitely.

These facts arose a number of problems that lay in the field of my interest and inspired my searching activity.

2. The *aim* of profound researching in the field of criminal law is with the usage of the methodology of criminal sciences.

This research has been done with an intention of *complexity* - that is the criminological aspects of these crimes, the analysis of their substantive and procedurals law problems.

It is from the complexity of my dissertation that it is dealing with two different *researching fields* of problems.On the one hand I intend to present the main trends of jurisdiction in other countries. On the other hand I give propositions about 'de lege ferenda' and criticize the 'de lege lata' in Hungary.

3. The *method* of my research is concentrated on comparative jurisprudence.

I cite from the law-making of more than twenty countries - legislation; jurisdiction; legal studies. My ambition was to show the main characteristics of the jurisdiction of the Continent.

The practicism of Anglo- Saxon law may also provide us with help in the subject.

I lay great stress on the Recommendations of the Council of Europe edited in 1990 ('Computer-related Crime') and in 1995 ('Concerning problems of criminal procedure law connected with information technology'). The significance of the former is in that it defines the delicta for the first time while the latter gives recommendations on the solving of a posteriori problems in criminal procedure law. Though the Recommendations do not bound Hungary they are still very progressive in the very (in this field) irksome harmonization of European criminal law. We must also remember that the basis of international criminal cooperation is the doctrine of 'double criminality'.

The *structure* of the thesis is divided into five bigger parts.

II. The summary of new scientific achievements

5. Criminological aspects:

This part of the thesis is rather descriptive. I try to give an overall elaboration and systemizing of all the literature available on the subject at the time of the writing.

5.1. The comprehensive criminological presentation of computer-relatid crimes is made rather difficult by the *latency* that is typical of these sorts of crimes. Banks

unfortunately counteract to investigation in cases of electronic attacks (computer-related fraud, misuse of credit-cards etc.).

The unauthorised reproduction or sale of computer programs, softwares, however, can also be hardly seen through.

5.2. The abuses related to computers go back to the time when computers appeared in the civil sphere. Already at the end of the 50's they committed manipulations with the intention of procuring an unlawful lucre. This may be regarded as typical even today.

The extent of damages of crimes against property committed with a computer significantly exceed the loss of damages caused by 'ordinary' delicta against property.

The unauthorised use of a protected program, the unauthorised reproduction of semiconductors and the putting of pornographic recordings on the internet can also be motivated by making profit. The misuse of credit- and telephone cards is tremendously growing.

In this section you can read about the Equity-Funding case, the Rifkin case and others that are well-known examples of the international literature.

5.3. The espionage of protected personal data, violation of state-, official-, commercial- and banking secrets is also typical.

5.4. With the development of computer nets the scope of crimes committable with the computer also widened. These can be of the most various sorts: offences against public calm (agitation against community, spreading of rumours, threatening with public menace etc.) occur newly on Internet, but drugs are also advertised here; we can find information on the know-how of bomb-making, on the maffia, the 'services' of extremist organizations and so on.

5.5. The most dangerous crime among computer abuses is *hacking*. Hackers break the integrity and policy of computer systems. The aim of unauthorised espionage can be teenage curiosity or access to business- or state secrets.

In the thesis you can read about those (West-)German young people who entered into the service of the KGB and 'broke into' the most protected US systems in the second half of the eighties; also you can read about the Kevin Mitnick and Kevin Poulsen cases.

With the building out of the computer-nets (extra-, intranet, Internet) the elctronic data basis got to be threatened *by anyone, from anywhere and at any time.*

5.6. Another feature of computer-related crimes is that the *speed* of its commitment makes it difficult to reveal them.

6. The possible answers given to the challenges concerning criminal policy and jurisdiction

6.1. I wish to illustrate the complexity of the challenge of jurisdiction and find the possible answers with the help of statements of eminent authors like Angyal Pál , Bárd Károly, Békés Imre, Farkas Ákos, Finkey Ferenc, Finszter Géza, Földvári József, Hacker Ervin, Kálmán Györgyi, Irk Albert, Irk Ferenc, Kertész Imre, Lévai Miklós, Merényi Kálmán, Nagy Ferenc, Pusztai László, Tokaji Géza, Tóth Mihály, Wiener A. Imre in Hungary and Karl Binding, Raymond Gassin, Michael Gemignani, Otto Harro, Henrik Kaspersen, Franz von Liszt, Peter Schick, Gabriele Schmölzer, Ulrich Sieber, Martin Wasik and others from abroad. At the same time *my ambition* is to show my point of view as well.

6.2. It is the duty of the government in power to organize the fight against delinquency and the provision of the necessary conditions. This may happen in accordance with the general political aims. The decisions of the government in the

field of criminal policy are restricted to a legal level by the material knowledge and conceptual system, also the legitimacy of jurisdiction.

We can read different opinions about the concept of criminal policy in the Hungarian legal literature. Some authors say that criminal policy hab a wider sense than criminal jurisdiction, because the former has to deal with averting as well. Others are of the opinion that in order to preserve the exact nature of research the concept of criminal policy should be limited to criminal legislature and application of law. This is what the thesis holds, too. No doubt that the scope of criminal policy extends the limits of judicature.

The forming of the national criminal policy is necessarily and more and more powerfully influenced by international law. National rights are the basis of the joining of the parts of the world in a material-productive, technical-technological way - and thus the basis of the approaching of criminal law. This latter - objective - process is strengthened by another sad objective phenomenon: the ever-growing international criminal tendency. It leads to the deepening of criminal cooperation. The *return* of our country amongst the well-developed, democratic countries of Europe demands that we accept and make part of the internal law those international norms that are recognised and followed in these countries. The norms of the International Treaty of Civil and Political Rights, the European Human Rights Convention, the Social Charta, other international documents and the decisions of the Human Rights Court form an integral part of Hungarian material and procedural law.

6.3. In the document of 1990 the Council of Europe sets up a 'minimal' and another'optional' list in which the the acts proposed to be criminalised are defined for the first time. The Recommendation published in 1995 gives proposition to the solving of problems that arise in the process of the criminal procedure. This field is influenced indirectly by the Data Protection Agreement of the Council of Europe in 1981.(No. 108) which served as a basis to the elaboration of the Data Protection Law in Hungary (1992. LXIII.)

6.4. Among the ways of behaviour that endanger the order of social coexistence, the reproduction and harmonic development of society, we can find those ones that have been present in penal laws with a relativ permanency. They protect the fundamental norms, interests and values of social coexistence (like life, physical wellbeing, health, honesty, property, sexual freedom, political power etc.).

Social-economic-political changes and/or technical-technological development, however, bring forth the necessity of the criminalisation of new ways of conduct or the reduction or elimination of penalty in several cases.

This latter cathegory includes computer-related cimes and violations of law that mean a challenge to jurisprudence owing to their special nature.

6.5. The specific feature of computer-related crimes is that their object of action is the invisible and immaterial electronic impulse of computer data. As for their content the data can be extremely various, their function diverse. They can designate pecuniary value, person-bound facts, texts, pictures, charts that serve as a basis for legal estimation etc. The data can be unlawfully spied out, modified; can be erased partly or wholly, altered, amended etc. These intervenings change the intended representation of the content of the data basis as well. This sort of alteration can cause *pecuniary loss*, can *infringe the private sphere* of the person concerned or can call forth other kinds of disadvantage to the person in connection with the data. The unlawful erasure of computerised data or any other way of hindering the computer data processing can *disable* telecommunication, other communication, manufacturing processes, financial proceedings, it can be suitable for the creation of hatred-arousing, pornographic, alarm-spreading texts, pictures etc.

With the unlawful collecting, usage, transfer of data the interests of the individual whose data are concerned are infringed.

Computer softwares are the logical series of algorythms that is able to perform operations with data. The creation and elaboration of these programs is an *intellectual activity.*

So *penal law* has to build out the protection of the *data as the carrier of large-scale information*, and also *data as a system, i.e. the program.*

6.6. Save for the last decades of the twentieth century jurisprudence concentrates on the protection of *objects with a physical existence* belonging to a (rightful) owner.

The unlawful seizure or damaging of these objects in various ways is sanctioned by the rules. These objects materialize for the outer world the assets to be protected.

In the course of the development of law the following attacks against property are generally sanctioned throughout the world with more or less the same meaning:

a./ unlawful seizure of someone else's property (stealing, robbing, blackmail),
b./ unlawful treatment of a stranger's property lawfully taken over (embezzlement),
c./ the giving over of someone's own property with a deceit (fraud),
d./ the damaging or destruction of someone else's property (nuisance) ..... and we could go on with the list.

6.7. Thus the scope of penal law - besides the protection of material objects objectivised has to be spread to the electronic impulses that cannot be seen, have no physical existance and only have a relevant content in the given circumstances.

Foreign legal literature deals more and more with the necessity of paradigm changes in penal law as the traditional doctrine and institutions of criminal protection of physical, perceptible objects cannot altogether be adapted in protection of electronic data.

My point of view is the following:

1./ *Chattels* with physical existance are dependant upon an owner or a rightful possessor, and all its partial legitimation (e.g. possession, usage) is damaged or put at risk at teh same time with the commitment of a 'traditional' crime.In the case of immaterial *data* the ownership cannot be realized. The total of rights does not only belong to the subject of the data but is distributed (the subject and the possessor of the data etc.) and the elements of this totality of rights are often opposed to or compete with each other.

2./ The *rights to information* are not similar (either in form or in content) to the exclusive competence of the owner or rightful possessor of the chattels.

Were it so the freedom of information flow would be hurt. In the course pf protection of computer data an extraordinarily subtle equilibrium has to be found between the subject and possessor, or the collector of data - and the interest of society in free information flow. The means of penal law have to be used to reach this aim.

3./ Computer data have meaning and along with this, value for the subject or collector of data, or any other possessor of information solely *in concrete circumstances, at a concrete time.* From these circumstances information can only be taken out, made use of or transmitted due to the interest of society. The unlawful spying out, manipulating, transmitting and usage of these information, however, infringes the interest of the subjects of the data in the first instance but finally of the society as a whole as well. New rules have to be created with regard to the points above.

6.8. An extremely important social-economic interest is safety, protection, undisturbance of process and technical conditions of computer data-processing and -transmission, the information treated there, that is growing, spreading and getting more and more significant nowadays - all in all the safeguarding of the integrity of computer data-processing and -transmitting systems.

In my opinion this is what we should regard as the *legal subject-matter* of computer-related crimes. From the diverse function of computer data-processing system follows that an attacj against these systems usually infringe other social relationships as well, thus computer-related crimes can be characterised with a *double legal object*; e.g. in the case of a computer fraud besides the safety and integrity of computer data-processing the propoerty conditions are also violated; or, through infringement of personal data the interest concerning the secrecy of personal data is also damaged. The common legal object can serve as a basis for an independent section, or sub-section, i.e. its title.

Scanning through international legislation we find the following ways of solving the problem:

- there are countries where this sort of crimes is placed collected in an independent law (e.g. in England the Computer Act was published in 1990), or in one section of the Special part (e.g. in France in Section III. of the Special Part of the Criminal Code).
- in other countries these crimes are defined besides the infringement of the traditional legal objects (e.g. Germany, Austria) or as a case of these (e.g. Sweden, Germany).

I believe that these delicta will shortly fit into the structure of the traditional Special part but after a certain time they will form an independent section of it.

The reason for this on the one hand is that their mutual legal object can be defined, on the otjer hand the criminal conduct of these crimes are the same (input, alteration, erasure or suppression of computer programs or data etc.).

Just remember the history of codifying traffic offences.

7. What I say is that in the focal point of informational crimes there is computer data, the means and aim of criminal deeds. I classify informatic infringements of law according to this as follows:

1./ Computer data as a means of crime:

a./ a direct means of data-manipulation that are committed with the aim of

- fraud;
- infringement (e.g. virus programs);
- sabotage (e.g. disturbing the work of communicational systems).

b./ An indirect means: creating and presenting of pornographic, racist, or other unlawful data files on the world net etc.

2./ Computer data as the aim of the crime:

- the unlawful spying out of personal, specifically personal, public data, also legally protectes

secrets (like data meant to be processed on the computer), making data available for an

unauthorised person etc.

- unauthorised interception of computer communication (e-mail, e-bussiness);
- the unauthorised use of programs (the copying, usage, forbidden trade of programs protected

by copyright etc.).

A special infringement of law is 'hacking' as this serves as a preparation ('fore-action') for the above mentioned crimes.

8. Certain types of crimes

8.1. For the legal classification of computer-related crimes we first have to get acquainted with the specific features and technical basis of certain criminal conducts. Then we can decide whether the given, concrete act can be fit into the conditions of an abstract case.

If - with the help of the well-known means of interpretation of law - we find that it is not possible, then (because of the garantiating doctrine of 'nullum crimen sine lege') there is a need for stating new facts of the case; but we have to count with the danger of doubling the facts of the case. We have to point out in advance that Hungarian legislation is a few steps back in the criminalization of some acts

(e.g. hacking, unlawful changing of data), but for example in the case of copyright protection decriminalization would be more useful.

8.2. By the infringement of operative copyright and neighbouring rights today in Hungary we have got ten thousands of potential computer criminals.

A rule created on political pressure cannot be kept. It is physically impossible to control every computer in the country to find out who runs illegally obtained programs on their machines.

The keeping up of extraordinarily high prices (loaded with extra profit) of computer programs should be revised for this is what mainly induces the infringements against computer programs. The unlawful usage, copying, trading of these is a typically cicil law problem.

Penal law should use its utmost stringency against the professional traders and duplicators of of computer programs. These forbidden acts infringe heavily the financial and marketing interestes of legal owners. The fight should be concentrated to this field.

Unfortunately the arguments against these facts are not of the professional kind.

8.3. The 'electronic break-in' into the memory of a computer or through it into any net as an unlawful input is in itself an infringement, but the real danger is in the conduct that may follow the entering. In this way data can be put in, altered, erased, financial transactions can be performed, viruses and other deteriorating programs can be intermitted, data stocks csn be copied, communication can be spied out etc.

Taking all this into account it seems justified to regard this sort of action an independent type of crime with *subsidiary* characteristics - similar to the Dutch example mentioned.

The 'electronic burglar' could only be responsible if he would not commit any other crimes (detailed below) with this act of his. An unlawful input de lege ferenda - concerning its severity - would not exceed the level of delinquency.

Finnish legislature is different from this, and my thesis gives a short description of that, too.

8.4. The notion of computer fraud is disputed until this very day not only in Hungary but in the legal literature of other countries as well.

The debate is about the role of computer as a means and also about whether there is a deceit of a natural person or not. In the crimonal codes of West-European countries computer fraud usually appears beside traditional deceit, or as a sub-case of it (Sweden, Finland); or as an independent presumption of facts. (Germany, Denmark, Austria).

Computer fraud has been a subject of criminal jurisdiction in Hungary since 1994 - and I have doubts about it.

A dilemma concerning the Sc. 300/A:

a./ The ruling of the definition and facts of case arises a debate on interpretation. The bill accentuated the aim and at the same time created a concept comcurring with traditional fraud. The accepted law renders the influencing of computer processing as a criminal conduct an offence.

b./ The nomination of the facts is 'computer fraud'- however, in the text not only fraud, but the elements of damage also take place. This creates a controversion between the title and the content. A solution could be later on (besides regulating the intellectual fights against computer fraud) there will be a new ruling for intellectual misuse of data as well. The latter criminal act is the 'inhibiting of computer data-processing and -transmission'.

c./ Paragraph (3) of Sc. 300/A concerns the unauthorised influencing of a special form of computer data-ptocessing. The usage of faked telephone-cards or SIM-cards can be regarded as a data input manipulation and the situation is the same with unauthorised changing of data on the chip of a mobile.

d./ The usage of a fake telephone card induces a series of other problems of legality. The forgery of a card is placed under Sc. (1) of 300/A,;while using it is dealt with in Sc. (3) of the same rule.

The 'non-case' regulated in paragraph (3) cannot really eliminate my doubts about the definiton of the systemizing computer crimes or the ruling of them.I think that forgery of telephone-cards and the multiplying of analogue mobileles clearly show the exact nature of these acts; namely data-manipulation with the intention of illegal profit-gaining.

Now I give suggestions de lege ferenda to the alteration of the ruling, to which I can see more alternatives:

- abrogation of paragraph (3) of Sc. 300/A of the Criminal Code ; there is no need to lay emphasis on any computer system;
- the recommendation from 1994 should be taken into consideration;
- common fraud cases (326§ CC) can be made adaptable for the evaluation of computer fraud with an'extension of interpretation.. (As it is done in Scandinavia.) The advantage of the latter is in the eliminating of the unceirtantiy - that usually occurs during the course of jurisdiction - when a computer is involved in a crime.

Another aspect could be the criminalizatin of manipulating 'simple computer systems' (phonecards, taxameters etc.) with the intent of illegal profit-making. (Cp. Sweden's regulations.)

In my opinion this would mean an 'over-regulation' in this subject and also aconsiderable uncertainty in what shuold be regarded a 'simple computer system' - as most probably a taxative legal listing is not possible.

8.5. Unauathorised data-changing as an ittellectual attack against comuter data-procesing.

The damage may occur in the partial or total erasure of the data; the formating [?] of the disc; the paralysing of the computer-processing activity or its overloading etc. Replacement of the data is also an expensive process.

The trend of legal regulation of the countries that I have examined shows that unauthorised changing of the data is either an individual (Austria, Switzerland) or a subsidiary (Italy) crime. This act has typically been place beside nuisance.

A new criminal statement in our Criminal Code would clearly mark the distinction that is 'mixed up' in the present 300/a §.

9. Answers given to the challenges to criminology

Analysing the above mentioned challenges I am looking for the answers with the help of the ideas of such authors (also eminent in the same field of criminal procedure and international criminal law), like Pál Angyal , Károly Bárd, Endre Bócz, Ervin Cséka, Géza Katona, Gusztáv Kautz, Imre Kertész, Tibor Király, Flórián Tremmel, Imre A. Wiener and Wolfgang Bär, Ulrich Sieber, Irini Vassiliki, Sir John Smith and others.

As there is a close connection between criminal substantive- and procedural law, the alteration in the one necesserily inflicts the other. Several problems arise from the 'invisible' and 'incorporeal' nature of computer data (as being electronic impulses) for substantional and procedural law alike.

In this part of the thesis the following questions are discussed:

a./ search,
b./ seizure
c./ eavesdropping,
d./ computer-data as a proof of evidence,
e./ the obligation of the accused and the witness for co-operation.

9.1. It would be conform to mention 'electronic data-processing systems' as possible objects of house search according to the 1995 Recommendation of European Council - de lege ferenda. This way of wording is important because electronic data-processing and -transmitting cannot be localized in space.

9.2. Analysing the question of seizure the main problem lies in deciding whether any data or data-processing means are seized. It is only possible to seize an object of proof - thus in this case the means of data-processing - but only if the object in question falls out from the possession of the accused.

It can only happen when the data are erased from the memory of the computer after being copied.

The authenticity of these data must serve as a guarantee for both the investigating authorities and the individual(s) concerned in the case.

I think that in connection with seizing computer data Hungarian criminal procedure law should be amended. With the necessary amendments certain guarantees seem to be inevitable.

De lege ferenda only the essential requirements are to be stated as to the visualizing the data that are needed for a judgement on the merit.

Furthermore it has to be ensured that no interest of individuals, companies or of anyone else would be infringed.

It seems to be justified that the playing and printing of the seized data-processing means should get under a prosecutor's control.

9.3. As far as interception is concerned I had to make it clear whether there is a legaly identifyable difference between the interception of data-processing means.

Legal practice in Europe is rather diffuse in this question.

Some countries (France, Great Britain) take out electronic data-processing forms; whilst others (Germany, the Netherlands) do not. In Hungary the law of 1994. XXXIV. §. 69. 1/c. provides about interception of telephones or any other telecommunicating systems that can substitute a telephone. It is to be decided whether the broadcasting of computer data-transmitting lines, radio frequencies and satellites belong to this category.

Based on the functioning of these data-processing means my thesis argues for the applicability of the Section above.

9.4. Where computer-data is examined as a proof I compare the British 'hearsay' rule of 1988 with the provisions of the Recommendation of the European Council.

The first question is whether a document printed by a computer can be used as a proof or not.

Some authors say yes - in case the printed document concerns a fact that has been observed and fixed by the computer. Another very similar case is where the printed document is the fact itself and that has to be proved. The crucial point is that the conpiter is functioning in several ways. Thus we can only decide whether a computer document may or may not be used as an evidence in the given case if we can see the technical outcome of the concrete deed.

The thesis then states that conclusive computer data can be realised for direct perception on a printed sheet or a photo made of the screen.

I regard this as a secondary proof ontologically - for these incriminated data are stored in the memory of a computer or other data-processing means.

9.5. My views about the obliged cooperation of the accused will surely be a subject of vehement dispute.

It requires consideration whether to raise the assistance of the accused in entering a computer, a net or files into the sphere of cooperating obligation.

The reason for this is the fact that entering a computer-system or a file can be made difficult or impossible and that makes the process very expensive.

It is possible, for example, that the extent of damage of a criminal act is not proportionate with the expeses of breaking up passwords or decoding secret documents. The accused cannot be forced to confess his/her deed. It would be contrary to Sc. 14/g of the international treaty about 'Civil and Political Rights'.

I hold that letting the investigating authorities know the data is not an admittance on behalf of the accused; for this evidence is not more than a small link in the chain of evidences.

At the moment by Hungarian law if the accused denies cooperation it may induce a coercion action like a house searching together with entering into a computer or a net.

10. International legal assistance

10.1. During the centuries several ways of international legal cooperation have developed.

The Sc. 5/1 of the Treaty of Strasbourg (1959) confirms that giving or getting legal assistance is possible only if the crime in question is indictable in both countries.

This fact in itself renders inevitable that Hungarian legislation should be made level with European legislation. International legal assistance may become of a special importance in forcing back offences through the Internet.

Until incitement and pornography is not indictable in every country of the world, the deletion of these phenomena is non-realistic.

10.2. Another very exciting problem is that of direct penetration. Namely, whether in the course a 'hot trace' investigation the authorities may follow a hacker on a foreign telecommunicating line or reach a foreign data-basis. In my opinion direct entering into other countries' communication system ought to be legalized - but only with the serious restriction that data information must not be made available, altered, copied etc.

11. On the utility of the thesis

Hungary is at a significant disadvantage when it comes to electronic data-processing. (It is enough to remember the 'Cocom-list' created against ex-socialist countries.)

Thus we were to face computer-related crime later in time. Technically more developed countries are much ahead of us in legislation, too. Besides the

Recommendations of the Council of Europe the above mentioned legislative solutions could serve for us as examples; not forgetting of course the traditions of Hungarian legislative practice.

Hungary is over the first phase of codifying informational crimes - very soon it will arrive at the second phase.

In my thesis there are ideas for the following problems:

- the identifying of the text of computer fraud and the exact place of it in the system;
- attack against computer computer data as a 'sabotage'; and
- criminalizing of forbidden trade, copying of chips;
- the extension and alteration of objective enforceable acts (i.e. house search, seizure, interception);
- thinking over the obliged cooperation of the parties involved in the criminal process;
- ensuring the strengthening of international legal assistance.

Concerning jurisprudence the thesis may give some practical advice on deciding conflicts between concurring statements in criminal substantive law by analyzing the role of the computer.

In criminal procedure law the questions concerning the effectiveness of investigating these crimes can be useful.

Together with amendments (concrete cases, technical descriptions etc.) the thesis could serve as a starting point for a special subject in the teaching of law.

The different forms of infringements can be informative for all those for whom the integrity of electronic data-processing is important; who work with computers; who use a telephone card; draw money by a bank card or pay with it.

All this information could be useful for crime-prevention.

My thesis tries to give an effective help in its complexity for the first time in Hungarian legal literature.

IRODALOMJEGYZÉK

Angyal Pál: A csalás. (A magyar büntetőjog kézikönyve 16. kötet). Budapest. 1939.

Angyal Pál: A lopás (A magyar büntetőjog kézikönyve 10. kötet). Budapest, 1932.

Angyal Pál: A titok védelme anyagi és alaki büntetőjogunkban. Budapest, 1908.

Balogh Zsolt György: Jogi informatika. Budapest - Pécs, 1998.

Bär, Wolfgang: Beschlagnahme von Computerdaten II. Computer und Recht, 12. 1996. 12. s.744-752.

Bequai, August: Computer Crime. Massachusetts. 1978.

Bércesi Zoltán: A szerzői jogi jogharmonizáció az Európai Közösségben, a computer - software termékek védelméről szóló irányelv hatásai a magyar szerzői jogban. Mągyar Jog 42. 1995. 7. 397-398.l.

Chambliss, William: Exploring Criminology. New York 1988.

Clark, Ramsey: Crime in America. New York, 1970.

Cornwall, Hugo: Data theft. London, 1990.

Cséka Ervin: A büntető ténymegállapítás elméleti alapjai. Budapest, 1968.

Erdősy Emil - Földvári József - Tóth Mihály: Magyar Büntetőjog, Különös rész. Budapest, 1998.

Farkas Ákos: A bűnözés okozta válság - a jogállami büntető igazságszolgáltatása válsága. Ünnepi tanulmányok II. Horváth Tibor 70. születésnapjára, Miskolc, 1997. 195.l.

Farkas Ákos: A kriminálpolitika és a büntető igazságszolgáltatás hatékonysága. Megjelent: Tanulmányok Szabó András 70. születésnapjára, Budapest 1998. 85.l.

Fenyvesi Csaba: Rendőrség és marketing. Pécs, 1974.

Finkey Ferenc: A magyar büntetőjog tankönyve. Budapest, 1914.

Finszter Géza: Európai rendészeti modellek és a magyar rendőrség. Megjelent: Kriminológiai Közlemények 57. Budapest 1999. 241.l.

Földvári József: Magyar Büntetőjog, Általános rész. Budapest, 1997.

Gassin, Raymond: Az informatika büntetőjoga, Magyar Jog 35. 1988. 2. 162-172.l.

Gemignani, Michael: Law and the Computer, Boston 1981.

Gönczöl Katalin - Korinek László - Lévai Miklós: Kriminológiai ismeretek Bűnözés - Bűnözéskontroll. Budapest, 1996.

Greve, Vagn: EDB-strafferet, Kopenhagen, 1986.

Hance, Oliver: Üzlet és jog az Interneten. Budapest, 1997.

Jaburek, Walter - Schmölzer, Gabriele: Computer - Kriminalität. Wien, 1985.

Kaspersen, H.W.K.: Computermisdaad en strafrecht. Antwerpen, 1986.

Katona Géza: A nyomok azonosítási vizsgálata a büntetőel járásban. Budapest, 1965.

Kautz Gusztáv: A magyar büntetőjog tankönyve. Budapest, 1881.

Kecskés László: EK jog és jogharmonizáció. Budapest, 1995.

Kertész Imre: A számítógépes hamisítás, Rendészeti Szemle XXI. 1993/4. 14.l.

Kertész Imre: Kép- és hangtechnikai eszközök a büntetőeljárásban, Emlékkönyv Dr. Cséka Ervin születésének 70. és oktatói munkásságának 25. évfordulójára, Szeged 1992. 324.l.

Király Tibor: Büntetőítélet a jog határán. Budapest, 1972.

Korinek László: Rejtett bűnözés. Budapest, 1988.

Lévai Miklós: Kábítószerek és bűnözés. Budapest, 1992.

Lloyd, Ian: Computer Crime, New Law Journal 08.08.1986. p(s). 761-762.

Nagy Tibor: A számítástechnika hatása a büntetőjogra. ÜÉ. 28. 1992. 2-3. 61-66.l.

Nagy Zoltán: A bankkártyával összefüggő visszaélések, Jura 4. 1997.2. 11-15.l.

Nagy Zoltán: A számítógépes bűncselekmények kódifikációjáról de lege lata és de lege ferenda, Belügyi Szemle 37. 1999. 11. 16-27.l.

Nagy Zoltán: A számítógépes bűnözés Computerworld - Számítástechnika 5. 1990.41. 16-19.l.

Nagy Zoltán: A számítógéppel elkövethető hamisításokról, Belügyi Szemle 35. 1997.3. 28-38.l.

Nagy Zoltán: A számítógéppel megvalósítható vagyoni jogsértésekről, Bűnügyi Műhelytanulmányok 1. 1992.1. 22-26.l.

Nagy Zoltán: A szerzői jog büntetőjogi védelméről, Computerworld Számítástechnika 8. 1993.18. 6.l.

Nagy Zoltán: Az elektronikus adatfeldolgozó- és adatátviteli rendszerek elleni támadás büntetőjogi értékeléséről, Magyar Jog 43. 1996. 10. 592-602.l.

Nagy Zoltán: Az informatika és a büntetőjog, Magyar Jog 38. 1991.1. 21-26.l.

Nagy Zoltán: Konferencia az információtechnikai bűnözésről, Magyar Jog 40. 1993.2. 102-105.l.

Nagy Zoltán: Törvénytervezet a számítógépes csalók ellen, Computerworld - Számítástechnika 8. 1993.22. 1. és 6.l.

Otto, Harro: Übungen im Strafrecht. Berlin - New York 1995

Pusztai László: Komputerbűnözés és a büntetőjogi reform az NSZK-ban, Magyar Jog 34. 1987.11.sz. 958.l.

Pusztai László: Számtógép és bűnözés. KKT. XXVI. kötet. Budapest, 1989. 85-146.

Rossa, Caroline Beatrix: Mißbrauch beim electronic cash. Computer und Recht, 13. 1997. 4. s. 219-226.

Sieber, Ulrich: Computerkriminalität und Informationsstrafrecht. Computer und Recht 11. 1995. 2. s.100-111.

Sieber, Ulrich: The International Emergence of Criminal Information Law. Köln - Berlin -Bonn - München 1992.

Siegler Eszter: A számítógéppel kapcsolatos és a számítógépes bűncselekmények, Magyar Jog 44. 1997. 12.sz. 741.l.

Tóth Mihály: Gazdasági bűncselekmények az alakuló joggyakorlatban. Budapest 1997.

Tremmel Flórián - Fenyvesi Csaba: Kriminalisztikai tankönyv és atlasz. Budapest-Pécs, 1998.

Tremmel Flórián: Büntető eljárásjog. Pécs, 1996.

Vassiliki, Irini: Multimediale Kriminalität. Computer und Recht 13. 1997. 5. s. 297.

Verebics János: A tér, a szabadság és a normák. www.Verebics J.-inet jog.htmViski László: Közlekedési büntetőjog. Budapest, 1974.

Wasik, Martin: Crime and the Computer, 1991.

Wiener A. Imre: A nemzetközi büntetőjog a nemzetközi jog aspektusából (Nyugat-európai hatások a magyar jogrendszer fejlődésében.) Budapest, 1994.

AZ EURÓPA TANÁCS IDEVONATKOZÓ AJÁNLÁSAI

Council of Europe: Recommendations No. R (89) 8 of the Committee of Ministers to Members States on Computer-related Crime. Council of Europe: Recommendations No. R (95) 14 of the Committe of Ministers to Members States on Concerning Problems of Criminal Procedure Law Connected with Information Technology.

Council of Europe: Recommendations No. R (99) 14 of the Committee of Ministers to Members States on Universal Community Service Concerning New Communication and Information Services.

Council of Europe: Recommendations No. R (99) 5 of the Committee of Ministers to Members States for the Protection of Privacy on the Internet.

RÖVIDÍTÉSEK JEGYZÉKE

Atv. = az 1992. évi LXIII. törvény a személyes adatok védelméről és közérdekű adatok nyilvánosságáról;

Btk. = az 1978. évi IV. törvény a Büntető törvénykönyvről;

Be. = az 1973. évi I. törvény a Büntető eljárásról;

Rtv. = az 1994. évi XXXIV. törvény a Rendőrségről;

NB. = az 1996. évi XXXVIII. törvény a Nemzetközi bűnügyi jogsegélyről;

ABH. = Alkotmánybírósági Határozatok;

BJD. = Büntetőjogi Döntvénytár;

BH. = Bírósági Határozatok;

CW-Sz.= Computerworld – Számítástechnika

BSz. = Belügyi Szemle

JK. = Jogtudományi Közlöny

KKT. = Kriminológiai és Kriminalisztikai Tanulmányok

MJ. = Magyar Jog;

RSz. = Rendészeti Szemle

ÜÉ. = Ügyészségi Értesítő

NÉV- ÉS TÁRGYMUTATÓ